10/069112

PCT/JPOO/05770

13.09.00

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: １９９９年１２月　３日

出願番号
Application Number: 平成１１年特許願第３４５２２９号

出願人
Applicant (s): 富士通株式会社
株式会社日立製作所
日本コロムビア株式会社
三洋電機株式会社

JP 00/05770

4

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

２０００年１０月２０日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号　出証特２０００－３０８５４４２

【書類名】　特許願

【整理番号】　1991488

【提出日】　平成11年12月 3日

【あて先】　特許庁長官殿

【国際特許分類】　H04M 11/08

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　畑中　正行

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　蒲田　順

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　畠山　卓久

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　長谷部　高行

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　小谷　誠剛

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　古田　茂樹

【発明者】
【住所又は居所】　東京都小平市上水本町５丁目２０番１号　株式会社日立製作所　半導体グループ内
【氏名】　木下　泰三
【発明者】
【住所又は居所】　東京都港区赤坂四丁目１４番１４号　日本コロムビア株式会社内
【氏名】　穴澤　健明
【発明者】
【住所又は居所】　大阪府守口市京阪本通２丁目５番５号　三洋電機株式会社内
【氏名】　日置　敏昭
【発明者】
【住所又は居所】　大阪府守口市京阪本通２丁目５番５号　三洋電機株式会社内
【氏名】　金森　美和
【発明者】
【住所又は居所】　大阪府守口市京阪本通２丁目５番５号　三洋電機株式会社内
【氏名】　堀　吉宏
【特許出願人】
【識別番号】　000005223
【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号
【氏名又は名称】　富士通株式会社
【特許出願人】
【識別番号】　000005108
【住所又は居所】　東京都千代田区神田駿河台４丁目６番地
【氏名又は名称】　株式会社日立製作所

【特許出願人】

【識別番号】　000004167

【住所又は居所】　東京都港区赤坂四丁目１４番１４号

【氏名又は名称】　日本コロムビア株式会社

【特許出願人】

【識別番号】　000001889

【住所又は居所】　大阪府守口市京阪本通２丁目５番５号

【氏名又は名称】　三洋電機株式会社

【代理人】

【識別番号】　100064746

【弁理士】

【氏名又は名称】　深見　久郎

【選任した代理人】

【識別番号】　100085132

【弁理士】

【氏名又は名称】　森田　俊雄

【選任した代理人】

【識別番号】　100091409

【弁理士】

【氏名又は名称】　伊藤　英彦

【選任した代理人】

【識別番号】　100096781

【弁理士】

【氏名又は名称】　堀井　豊

【先の出願に基づく優先権主張】

【出願番号】　平成11年特許願第241747号

【出願日】　平成11年 8月27日

【手数料の表示】

【予納台帳番号】　008693

【納付金額】　　21,000円

【提出物件の目録】

【物件名】　　明細書　1

【物件名】　　図面　1

【物件名】　　要約書　1

【プルーフの要否】　　要

【書類名】　明細書

【発明の名称】　データ配信システム

【特許請求の範囲】

【請求項１】　コンテンツデータ供給装置から、暗号化コンテンツデータを複数のユーザの各端末に配信するためのデータ配信システムであって、

前記コンテンツデータ供給装置は、

外部との間でデータを授受するための第１のインターフェース部と

前記暗号化コンテンツデータの通信ごとに更新される第１の共通鍵を生成する第１のセッションキー発生部と、

前記ユーザの端末に対応して予め定められた第１の公開暗号化鍵により前記第１の共通鍵を暗号化して前記第１のインターフェース部に与えるためのセッションキー暗号化部と、

前記第１の共通鍵により暗号化されて返信されるデータを復号するためのセッションキー復号部と、

前記暗号化コンテンツデータを復号するためのライセンスキーを、前記セッションキー復号部により復号されたデータを鍵データとして暗号化するための第１のライセンスデータ暗号化処理部と、

前記第１のライセンスデータ暗号化処理部の出力を第２の共通鍵でさらに暗号化して前記第１のインターフェース部に与え配信するための第２のライセンスデータ暗号化処理部とを備え、

各前記端末は、

外部との間でデータを授受するための第２のインターフェース部と、

前記暗号化コンテンツデータを受けて格納する配信データ解読部とを備え、

前記配信データ解読部は、

前記第１の公開暗号化鍵によって暗号化されたデータを復号化するための第１の秘密復号鍵を保持する第１の鍵保持部と、

前記第１の公開暗号化鍵によって暗号化された前記第１の共通鍵を受けて、復号処理するための第１の復号処理部と、

第２の公開暗号化鍵を保持するための第２の鍵保持部と、

前記第２の公開暗号化鍵を、前記第１の共通鍵に基づいて暗号化し、前記第２のインターフェース部に出力するための第１の暗号化処理部と、

前記第２のライセンスデータ暗号化処理部からの暗号化されたライセンスキーを受け、前記第２の共通鍵に基づいて復号化するための第２の復号処理部と、

前記第２の復号処理部の出力を受けて、格納するための第１の記憶部と、

前記第２の公開暗号化鍵によって暗号化されたデータを復号化するための第２の秘密復号鍵を保持する第３の鍵保持部と、

前記第１の記憶部に格納されたデータに基づいて、前記第２の秘密復号鍵により前記ライセンスキーを復号するための第３の復号処理部とを備える、データ配信システム。

【請求項２】　前記配信データ解読部は、前記端末に着脱可能なメモリカードであり、

前記第１の秘密復号鍵は、前記メモリカードの種類に対応して予め定められた鍵であり、

前記第２の秘密復号鍵は、前記メモリカードごとに異なる、請求項１記載のデータ配信システム。

【請求項３】　前記第２および第３の復号処理部は、前記コンテンツデータ供給装置において前記第２の公開暗号化鍵で暗号化され、さらに前記第２の共通鍵で暗号化されて、前記ライセンスキーとともに配信されるライセンス情報データを前記第２のインターフェース部を介して受け、前記第２の共通鍵および前記第２の秘密復号鍵に基づいて復号し、

前記配信データ解読部は、

復号された前記ライセンス情報データを格納する第２の記憶部をさらに備える、請求項２記載のデータ配信システム。

【請求項４】　前記第１の共通鍵と前記第２の共通鍵とは、前記暗号化コンテンツデータの通信の際に、前記第１のセッションキー発生部により生成された同一の鍵データである、請求項３記載のデータ配信システム。

【請求項５】　前記第１の記憶部は、前記ライセンスキーに基づいて復号できる前記暗号化コンテンツデータを前記コンテンツデータ供給装置から受けて格

納し、

前記配信データ解読部は、

外部から指示される再生動作モードに応じて、前記第２の記憶部に格納されたライセンス情報データにより再生可能かを判断して、前記配信データ解読部の動作を制御するための制御部をさらに備え、

前記第１の暗号化処理部は、前記制御部に制御されて、前記コンテンツデータの再生動作が指示されるのに応じて、前記第３の復号処理部からの前記ライセンスキーを受けて、第３の共通鍵に基づいて暗号化して出力し、

前記第１の記憶部は、前記制御部に制御されて、前記コンテンツデータの再生動作が指示されるのに応じて、前記暗号化コンテンツデータを出力し、

各前記端末は、

前記暗号化コンテンツデータの通信ごとに更新される前記第３の共通鍵を生成する第２のセッションキー発生部と、

前記配信データ解読部からの前記第３の共通鍵により暗号化された前記ライセンスキーを受けて復号して抽出し、前記第１の記憶部から出力された前記暗号化コンテンツデータを前記ライセンスキーにより復号して再生するコンテンツデータ再生部とをさらに備える、請求項４記載のデータ配信システム。

【請求項６】　前記配信データ解読部は、

外部から指示される他の端末に前記暗号化コンテンツキーおよび前記ライセンス情報データを移転するための移動動作モードに応じて、前記配信データ解読部の動作を制御するための制御部と、

第３の公開暗号化鍵で暗号化処理を行なうための第２の暗号化処理部とをさらに含み、

前記第２の復号処理部は、前記制御部に制御されて、前記移動動作モードが指定されるのに応じて、前記第３の共通鍵に基づいて暗号化されて前記他の端末の側から送信される前記第３の公開暗号化鍵を復号して抽出し、

前記第２の暗号化処理部は、前記移動動作モードが指定されるのに応じて、前記ライセンスキーおよび前記ライセンス情報データを前記第３の公開暗号化鍵で暗号化し、

前記第１の暗号化処理部は、前記第２の暗号化処理部の出力を受けて、前記第３の共通鍵に基づいて暗号化して前記第２のインターフェース部に与え、

前記制御部は、前記移動動作モードが指定されるのに応じて、前記第２の記憶部に格納されている前記ライセンス情報データを消去し、

前記第１の記憶部は、前記移動動作モードが指定されるのに応じて、前記暗号化コンテンツデータを前記第２のインターフェース部に与える、請求項５記載のデータ配信システム。

【請求項７】　前記配信データ解読部は、

外部から指示される他の端末に前記暗号化コンテンツデータを移転するための複製動作モードに応じて、前記配信データ解読部の動作を制御するための制御部をさらに含み、

前記第１の記憶部は、前記複製動作モードが指定されるのに応じて、前記暗号化コンテンツデータを前記第２のインターフェース部に与える、請求項５記載のデータ配信システム。

【請求項８】　前記配信データ解読部は、

前記第２の共通鍵を生成するための第３のセッションキー発生部と、

前記第３のセッションキー発生部の出力を暗号化して前記第２のインターフェース部に与えることが可能な第３の暗号化処理部とをさらに含む、請求項３記載のデータ配信システム。

【請求項９】　前記第１の記憶部は、前記ライセンスキーに基づいて復号できる前記暗号化コンテンツデータを前記コンテンツデータ供給装置から受けて格納し、

前記配信データ解読部は、

外部から指示される再生動作モードに応じて、前記第２の記憶部に格納されたライセンス情報データにより再生可能かを判断して、前記配信データ解読部の動作を制御するための制御部をさらに備え、

前記第３の暗号化処理部は、第４の公開暗号化鍵により前記第３のセッションキー発生部の出力を暗号化して前記第２のインターフェース部に与え、

前記第１の暗号化処理部は、前記制御部に制御されて、前記コンテンツデータ

の再生動作が指示されるのに応じて、前記第３の復号処理部からの前記ライセンスキーを受けて、第３の共通鍵に基づいて暗号化して出力し、

前記第１の記憶部は、前記制御部に制御されて、前記コンテンツデータの再生動作が指示されるのに応じて、前記暗号化コンテンツデータを出力し、

各前記端末は、

前記暗号化コンテンツデータの通信ごとに更新される前記第３の共通鍵を生成する第２のセッションキー発生部と、

前記第４の公開暗号化鍵を前記配信データ解読部に与える公開鍵保持部と、

前記第４の公開暗号化鍵で暗号化された前記第２の共通鍵を復号可能な公開鍵復号部と、

前記配信データ解読部からの前記第３の共通鍵により暗号化された前記ライセンスキーを受けて復号して抽出し、前記第１の記憶部から出力された前記暗号化コンテンツデータを前記ライセンスキーにより復号して再生するコンテンツデータ再生部とをさらに備える、請求項８記載のデータ配信システム。

【請求項１０】　前記配信データ解読部は、

外部から指示される他の端末に前記暗号化コンテンツデータおよび前記ライセンス情報データを移転するための移動動作モードに応じて、前記配信データ解読部の動作を制御するための制御部と、

第３の公開暗号化鍵で暗号化処理を行なうための第２の暗号化処理部とをさらに含み、

前記第２の復号処理部は、前記制御部に制御されて、前記移動動作モードが指定されるのに応じて、前記第３の共通鍵に基づいて暗号化されて前記他の端末の側から送信される前記第３の公開暗号化鍵を復号して抽出し、

前記第２の暗号化処理部は、前記移動動作モードが指定されるのに応じて、前記ライセンスキーおよび前記ライセンス情報データを前記第３の公開暗号化鍵で暗号化し、

前記第１の暗号化処理部は、前記第２の暗号化処理部の出力を受けて、前記第３の共通鍵に基づいて暗号化して前記第２のインターフェース部に与え、

前記制御部は、前記移動動作モードが指定されるのに応じて、前記第２の記憶

部に格納されている前記ライセンス情報データを消去し、

前記第１の記憶部は、前記移動動作モードが指定されるのに応じて、前記暗号化コンテンツデータを前記第２のインターフェース部に与える、請求項９記載のデータ配信システム。

【請求項１１】　前記配信データ解読部は、

外部から指示される他の端末に前記暗号化コンテンツデータを移転するための複製動作モードに応じて、前記配信データ解読部の動作を制御するための制御部をさらに含み、

前記第１の記憶部は、前記複製動作モードが指定されるのに応じて、前記暗号化コンテンツデータを前記第２のインターフェース部に与える、請求項９記載のデータ配信システム。

【請求項１２】　前記第１のインターフェース部と前記第２のインターフェース部とは、携帯電話網により接続され、

前記コンテンツデータ供給装置は、

前記第１の公開暗号鍵に基づいて、前記ユーザの認証を行なう、請求項１記載のデータ配信システム。

【請求項１３】　前記第１のインターフェース部は、

前記端末と直接接続可能なコネクタ部を含む、請求項１記載のデータ配信システム。

【請求項１４】　前記第１のインターフェース部は、

前記メモリーカードと直接接続可能な接続部を含む、請求項２記載のデータ配信システム。

【請求項１５】　コンテンツデータ供給装置から、暗号化コンテンツデータと前記暗号化データを復号するためのコンテンツキーとのうちの少なくとも１つを複数のユーザの各端末に配信するためのデータ配信システムであって、

前記コンテンツデータ供給装置は、

外部との間でデータを授受するための第１のインターフェイス部と、

前記暗号化コンテンツデータの通信ごとに更新される第１の共通鍵を生成する第１のセッションキー発生部と、

前記ユーザの端末に対応して予め定められた第１の公開暗号化鍵により前記第１の共通鍵を暗号化して前記第１のインターフェイス部に与えるためのセッションキー暗号化処理部と、

前記第２の共通鍵により暗号化されて返信される第２の共通鍵と第２の公開暗号化鍵を復号し抽出するセッションキー復号部と、

前記暗号化コンテンツデータを復号するためのコンテンツキーを、前記セッションキー復号部により復号された第２の公開暗号化鍵により暗号化するための第１のライセンスデータ暗号化処理部と、

前記第１のライセンスデータ暗号化処理部の出力を前記第２の共通鍵でさらに暗号化して前記第１のインターフェイス部に与え配信するための第２のライセンス暗号化処理部とを備え、

各前記端末は、

外部との間でデータを授受するための第２のインターフェイス部と、

前記暗号化コンテンツデータおよび前記コンテンツキーを受けて格納する配信データ解読部とを備え、

前記配信データ解読部は、

前記第１の公開暗号化鍵によって暗号化されたデータを復号化するための第１の秘密復号鍵を保持する第１の鍵保持部と、

前記第１の公開暗号化鍵によって暗号化された前記第１の共通鍵を受けて、復号処理するための第１の復号処理部と、

第２の公開暗号化鍵を保持するための第２の鍵保持部と、

第２の共通鍵を生成する第２のセッションキー発生部と、

前記第２の公開暗号化鍵と前記第２の共通鍵を、前記第１の共通鍵に基づいて暗号化し、前記第２のインターフェイス部に出力するための第１の暗号化処理部と、

前記第２のライセンスデータ暗号化処理部からの暗号化されたコンテンツキーを受け、前記第２の共通鍵に基づいて復号するための第２の復号処理部と、

前記第２の復号処理部の出力と、前記コンテンツキーにて復号可能な暗号化コンテンツデータを格納するための記憶部と、

前記第２の公開暗号化鍵によって暗号化されたデータを復号化するための第２の秘密復号鍵を保持する第３の鍵保持部と、

前記記憶部に格納されたデータに基づいて、前記第２の秘密復号鍵により前記コンテンツキーを復号し抽出するための第３の復号処理部と、

前記第１の公開暗号化鍵を少なくとも含む第１の認証データを公開認証鍵により復号できるように暗号化して保持し外部に出力可能な第１の認証データ保持部と、

前記公開認証鍵により復号できる外部から与えられる第１の認証データを復号して抽出するための第１の認証復号処理部とを備え、

前記コンテンツデータ供給部は、

前記第１の認証復号処理部により抽出された前記第１の認証データに基づいて認証処理を行ない、少なくともコンテンツキーを配信するか否かを判断する配信制御手段をさらに含む、データ配信システム。

【請求項１６】　前記配信データ解読部は、前記端末に着脱可能なメモリカードであり、

前記第１の秘密復号鍵は、前記メモリカードの種類の対応して予め定められた値であり

前記第２の秘密複号鍵は、前記メモリカードごとに異なる、請求項１５記載のデータ配信システム。

【請求項１７】　各前記端末は、コンテンツ再生部をさらに備え、

前記コンテンツ再生部は、

予め定められた第３の公開暗号鍵を少なくとも含む第２の認証データを前記公開認証鍵に基づいて復号できるように暗号化して保持し、外部に対して出力できる第２の認証データ保持部をさらに含む、請求項１５記載のデータ配信システム。

【請求項１８】　前記第１の認証復号処理部は、

前記公開認証鍵により復号できるよう暗号化された第２の認証データをさらに復号して出力し、

前記配信制御部は、

前記第１の認証復号処理部にて抽出された前記第１の認証データおよび前記第２の認証データに基づいて認証処理を行ない、少なくともコンテンツキーを配信するか否かを判断する、請求項１７に記載のデータ配信システム。

【請求項１９】　前記第１のインタフェイス部と前記第２のインタフェイス部とは、携帯電話網により接続される、請求項１５記載のデータ配信システム。

【請求項２０】　前記第１のインタフェイス部は、

前記端末と直接接続可能なコネクタ部を含む、請求項１５記載のデータ配信システム。

【請求項２１】　前記第１のインタフェイス部は、

前記データ格納部と直接接続可能な接続部を含む、請求項１６記載のデータ配信システム。

【請求項２２】　前記データ解読部は、

前記接続部からのデータを受ける複数の端子を含み、

外部からの指令に従って、前記接続部からデータを受ける端子数が切換え可能である、請求項２１記載のデータ配信システム。

【請求項２３】　前記データ再生部は、

前記第３の公開暗号鍵にて暗号化されたデータを復号する第３の秘密復号鍵を保持するための第４の鍵保持部と、

外部にて前記第３の公開暗号化鍵によって暗号化された第２の共通鍵を復号し抽出するための第３の復号処理部と、

第３の共通鍵を生成する第３のセッションキー発生部と、

前記第３の復号処理部にて復号し抽出した前記第２の共通鍵に基づいて、前記第３の共通鍵を暗号化し出力するための第２の暗号化処理部と、

外部にて前記第３の共通鍵に基づいて暗号化されたコンテンツキーを復号し抽出するための第４復号処理部と、

前記記録部に記録された暗号化コンテンツデータを抽出した前記コンテンツキーにて復号し、再生するためのデータ再生部とをさらに備え、

配信データ解読部は、

前記公開認証鍵により復号できる前記コンテンツ再生部からの与えられる暗号

化された第２の認証データを復号して前記第３の公開鍵を抽出するための第２の認証復号処理部と、

前記第２のセッションキー発生部にて生成した第２の共通鍵を前記第３の公開暗号化鍵に基づいて暗号化する第３の暗号化処理部と、

前記データ再生部にて前記第２の共通鍵にて暗号化された前記第３の共通鍵を受けて、前記第１の復号処理部にて前記第２の共通鍵に基づいて復号した前記第３の共通鍵に基づいて、前記記録部に格納されたデータを前記第２の秘密復号鍵にて復号した前記コンテンツキーを、前記第１の暗号化処理部にて暗号化し、前記コンテンツ再生部へ出力を指示する制御部とをさらに備え、

前記制御手段は、前記第２の認証復号処理部により復号された前記第２の認証データに基づいて認証処理を行ない、少なくともコンテンツキーを出力するか否かを判断する、請求項１７記載のデータ配信システム。

【請求項２４】　前記配信データ解読部は、

前記第２の公開鍵によって前記第２の共通鍵を暗号化するための第４の暗号化処理部をさらに含み、

前記認証復号処理部は、外部から指示される、他の配信データ解読部に少なくとも前記コンテンツキーを移転する移動処理に応じて、前記他のデータ解読部の前記公開認証鍵によって復号できる暗号化された第１の認証データを、前記公開認証鍵にて復号して、前記他のデータ解読部における第１の公開暗号化鍵を抽出し、

前記第２のセッションキー発生部は、前記移動処理に応じて、前記第２の共通鍵を発生し、

前記第３の暗号化処理部は、前記移動処理に応じて、前記他の配信データ解読部の第１の公開暗号化鍵に基づいて、前記第２の共通鍵を暗号化し、

前記第２の復号処理部は、前記移動処理に応じて、前記他の配信データ解読部から前記第２の共通鍵によって暗号化され、入力される第４の共通鍵と他の配信データ解読部の第２の公開暗号化鍵とを復号して抽出し、

前記第３の復号処理部は、前記移動処理に応じて、第２の秘密復号鍵に基づいて、前記記録部に格納された第２の公開暗号化鍵にて暗号化されたデータを復号

し、コンテンツキーを抽出し、

前記第４の暗号化処理部は、前記移動処理に応じて、前記他のメモリカードの第２の公開暗号化鍵に基づいて、抽出された前記コンテンツキーを暗号化し、

前記第１の暗号化処理部は、前記移動処理に応じて、前記第４の暗号化処理部の出力を前記第４の共通鍵にて暗号化し、前記他の配信データ解読部に対して出力し、

前記制御手段は、前記第２の認証復号処理部により抽出された前記他のデータ解読部から出力された第２の認証データに基づき認証処理を行ない、少なくともコンテンツキーを出力するか否かを判断する、請求項１６記載のデータ配信システム。

【請求項２５】　前記配信データ解読部は、

前記認証復号処理は、外部から指示される、他の配信データ解読部から少なくとも前記コンテンツキーを移転する移動受理処理に応じて、前記第２の認証データ保持部が前記第２の認証データを出力し、

前記第１の復号処理部は、前記移動受理処理に応じて、前記他の配信データ解読部から前記第１の公開暗号化鍵によって暗号化され、入力される前記他の配信データ解読部にて発生された前記第４の共通鍵を復号して抽出し、

前記第２のセッションキー発生部は、前記移動受理処理に応じて、第２の共通鍵を発生し、

前記第１の暗号化処理部は、前記移動受理処理に応じて、第４の共通鍵に基づいて、前記第２の公開暗号化鍵と前記第２の共通鍵とを暗号化して出力し、

前記第２の復号処理部は、前記他の配信データ解読部に前記第２の公開暗号化鍵にて暗号化され、さらに前記第２の共通鍵にて暗号化されたコンテンツキーを前記第２の共通鍵にて復号し、前記記録部に記録する請求項２２記載のデータ配信システム。

【請求項２６】　前記コンテンツデータ供給装置は、

前記コンテンツ再生部と共通な第５の共通鍵を保持する第５の鍵保持部と、

前記第５の鍵保持部に保持された前記第５の共通鍵に基づいて、前記コンテンツキーを暗号化し前記第１のライセンス暗号化処理部に対して出力する第３のラ

イセンス暗号化部をさらに含み、

前記コンテンツ再生部は、

前記第５の共通鍵を保持する第６の鍵保持手段と、

前記第４の復号処理部と前記データ再生部との間に設けられ、前記第６の鍵保持部に保持された前記第５の共通鍵によって、前記第４の復号処理部の出力から前記コンテンツキーを復号し抽出し、前記データ再生部に対して出力する第５の復号処理部をさらに含む、請求項２１記載のデータ配信システム。

【請求項２７】　前記コンテンツデータ供給装置は、

前記コンテンツ再生部にて復号可能な第４の公開暗号化鍵を保持する第５の鍵保持部と、

第４の公開暗号化鍵に基づいて前記コンテンツキーを暗号化し前記第１のライセンス暗号化処理部にて出力する第３のライセンス暗号化部をさらに含み、

前記コンテンツ再生部は、

第４の公開暗号化鍵によって暗号化されたデータを復号できる第４の秘密復号鍵を保持する第６の鍵保持手段と、

前記第４の復号処理部と前記データ再生部との間に設けられ、第４の秘密復号鍵によって前記第４の復号処理部の出力から前記コンテンツキーを復号し抽出し、前記データ再生部に対して出力する第５の復号処理部をさらに含む、請求項２１記載のデータ配信システム。

【請求項２８】　前記データ再生部は、

複数の配信データ解読部を備える、請求項１６記載のデータ配信システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、携帯電話等の端末に対して情報を配送するためのデータ配信システムに関し、より特定的には、コピーされた情報に対する著作権保護を可能とするデータ配信システムに関するものである。

【０００２】

【従来の技術】

近年、インターネット等の情報通信網等の進歩により、携帯電話等を用いた個人向け端末により、各ユーザが容易にネットワーク情報にアクセスすることが可能となっている。

【０００３】

このような情報通信においてはデジタル信号により情報が伝送される。したがって、たとえば上述のような情報通信網において伝送された音楽や映像情報を各個人ユーザがコピーした場合でも、そのようなコピーによる音質や画質の劣化をほとんど生じさせることなく、情報のコピーを行なうことが可能である。

【０００４】

したがって、このような情報通信網上において、音楽情報や画像情報等の著作権の存在する創作物が伝達される場合、適切な著作権保護のための方策が取られていないと、著しく著作権者の権利が侵害されてしまうおそれがある。

【０００５】

一方で、著作権保護の目的を最優先して、急拡大するデジタル情報通信網を介して著作物データの配信を行なうことができないとすると、基本的には、著作物の複製に際して一定の著作権料を徴収することが可能な著作権者にとっても、かえって不利益となる。

【０００６】

ここで、上述のようなデジタル情報通信網を介した配信ではなく、デジタル情報を記録した記録媒体を例にとって考えてみると、通常販売されている音楽情報を記録したＣＤ（コンパクトディスク）については、ＣＤから光磁気ディスク（ＭＤ等）への音楽データのコピーは、当該コピーした音楽を個人的な使用に止める限り原則的には自由に行なうことができる。ただし、デジタル録音等を行なう個人ユーザは、デジタル録音機器自体やＭＤ等の媒体の代金のうちの一定額を間接的に著作権者に対して補償金として支払うことになっている。

【０００７】

しかも、ＣＤからＭＤへデジタル信号である音楽情報をコピーした場合、これらの情報がコピー劣化のほとんどないデジタル情報であることに鑑み、１つのＭＤからさらに他のＭＤに音楽データをデジタル情報としてコピーすることは、著

作権者保護のために機器の構成上できないようになっている。

【０００８】

すなわち、現状においては、デジタル記録媒体であるＣＤからＭＤへのコピーは、親から子へのコピーは自由に行なうことができるものの、記録可能なＭＤからＭＤへのコピーを行なうことはできない。

【０００９】

【発明が解決しようとする課題】

そのような事情からも、音楽データや画像データをデジタル情報通信網を通じて公衆に配信することは、それ自体が著作権者の公衆送信権による制限を受ける行為であるから、著作権保護のための十分な方策が講じられる必要がある。

【００１０】

この場合、情報通信網を通じて公衆に送信される著作物データを、本来受信する権限のないユーザが受信することを防止する必要があるのはもちろんのこと、仮に権限を有するユーザが受信を行なった場合でも、一度受信された著作物が、さらに勝手に複製されることを防止することも必要となる。

【００１１】

本発明は、上記のような問題点を解決するためになされたものであって、その目的は、情報通信網、たとえば携帯電話等の情報通信網を介して著作物データを配信する場合に、正当なアクセス権を有するユーザのみがこのような情報を受信することが可能な情報配信システムを提供することである。

【００１２】

この発明の他の目的は、配信された著作物データが、著作権者の許可なく複製されることを防止することが可能な情報配信システムを提供することである。

【００１３】

【課題を解決するための手段】

請求項１記載のデータ配信システムは、コンテンツデータ供給装置から、暗号化コンテンツデータを複数のユーザの各端末に配信するためのデータ配信システムであって、コンテンツデータ供給装置は、外部との間でデータを授受するための第１のインターフェース部と暗号化コンテンツデータの通信ごとに更新される

第１の共通鍵を生成する第１のセッションキー発生部と、ユーザの端末に対応して予め定められた第１の公開暗号化鍵により第１の共通鍵を暗号化して第１のインターフェース部に与えるためのセッションキー暗号化部と、第１の共通鍵により暗号化されて返信されるデータを復号するためのセッションキー復号部と、暗号化コンテンツデータを復号するためのライセンスキーを、セッションキー復号部により復号されたデータを鍵データとして暗号化するための第１のライセンスデータ暗号化処理部と、第１のライセンスデータ暗号化処理部の出力を第２の共通鍵でさらに暗号化して第１のインターフェース部に与え配信するための第２のライセンスデータ暗号化処理部とを備え、各端末は、外部との間でデータを授受するための第２のインターフェース部と、暗号化コンテンツデータを受けて格納する配信データ解読部とを備え、配信データ解読部は、第１の公開暗号化鍵によって暗号化されたデータを復号化するための第１の秘密復号鍵を保持する第１の鍵保持部と、第１の公開暗号化鍵によって暗号化された第１の共通鍵を受けて、復号処理するための第１の復号処理部と、第２の公開暗号化鍵を保持するための第２の鍵保持部と、第２の公開暗号化鍵を、第１の共通鍵に基づいて暗号化し、第２のインターフェース部に出力するための第１の暗号化処理部と、第２のライセンスデータ暗号化処理部からの暗号化されたライセンスキーを受け、第２の共通鍵に基づいて復号化するための第２の復号処理部と、第２の復号処理部の出力を受けて、格納するための第１の記憶部と、第２の公開暗号化鍵によって暗号化されたデータを復号化するための第２の秘密復号鍵を保持する第３の鍵保持部と、第１の記憶部に格納されたデータに基づいて、第２の秘密復号鍵によりライセンスキーを復号するための第３の復号処理部とを備える。

【００１４】

請求項２記載のデータ配信システムは、請求項１記載のデータ配信システムの構成に加えて、配信データ解読部は、端末に着脱可能なメモリカードであり、第１の秘密復号鍵は、メモリカードの種類に対応して予め定められた鍵であり、第２の秘密復号鍵は、メモリカードごとに異なる。

【００１５】

請求項３記載のデータ配信システムは、請求項２記載のデータ配信システムの

構成に加えて、第２および第３の復号処理部は、コンテンツデータ供給装置において第２の公開暗号化鍵で暗号化され、さらに第２の共通鍵で暗号化されて、ライセンスキーとともに配信されるライセンス情報データを第２のインターフェース部を介して受け、第２の共通鍵および第２の秘密復号鍵に基づいて復号し、配信データ解読部は、復号されたライセンス情報データを格納する第２の記憶部をさらに備える。

【００１６】

請求項４記載のデータ配信システムは、請求項３記載のデータ配信システムの構成に加えて、第１の共通鍵と第２の共通鍵とは、暗号化コンテンツデータの通信の際に、第１のセッションキー発生部により生成された同一の鍵データである。

【００１７】

請求項５記載のデータ配信システムは、請求項４記載のデータ配信システムの構成に加えて、第１の記憶部は、ライセンスキーに基づいて復号できる暗号化コンテンツデータをコンテンツデータ供給装置から受けて格納し、配信データ解読部は、外部から指示される再生動作モードに応じて、第２の記憶部に格納されたライセンス情報データにより再生可能かを判断して、配信データ解読部の動作を制御するための制御部をさらに備え、第１の暗号化処理部は、制御部に制御されて、コンテンツデータの再生動作が指示されるのに応じて、第３の復号処理部からのライセンスキーを受けて、第３の共通鍵に基づいて暗号化して出力し、第１の記憶部は、制御部に制御されて、コンテンツデータの再生動作が指示されるのに応じて、暗号化コンテンツデータを出力し、各端末は、暗号化コンテンツデータの通信ごとに更新される第３の共通鍵を生成する第２のセッションキー発生部と、配信データ解読部からの第３の共通鍵により暗号化されたライセンスキーを受けて復号して抽出し、第１の記憶部から出力された暗号化コンテンツデータをライセンスキーにより復号して再生するコンテンツデータ再生部とをさらに備える。

【００１８】

請求項６記載のデータ配信システムは、請求項５記載のデータ配信システムの

構成に加えて、配信データ解読部は、外部から指示される他の端末に暗号化コンテンツキーおよびライセンス情報データを移転するための移動動作モードに応じて、配信データ解読部の動作を制御するための制御部と、第３の公開暗号化鍵で暗号化処理を行なうための第２の暗号化処理部とをさらに含み、第２の復号処理部は、制御部に制御されて、移動動作モードが指定されるのに応じて、第３の共通鍵に基づいて暗号化されて他の端末の側から送信される第３の公開暗号化鍵を復号して抽出し、第２の暗号化処理部は、移動動作モードが指定されるのに応じて、ライセンスキーおよびライセンス情報データを第３の公開暗号化鍵で暗号化し、第１の暗号化処理部は、第２の暗号化処理部の出力を受けて、第３の共通鍵に基づいて暗号化して第２のインターフェース部に与え、制御部は、移動動作モードが指定されるのに応じて、第２の記憶部に格納されているライセンス情報データを消去し、第１の記憶部は、移動動作モードが指定されるのに応じて、暗号化コンテンツデータを第２のインターフェース部に与える。

【００１９】

請求項７記載のデータ配信システムは、請求項５記載のデータ配信システムの構成に加えて、配信データ解読部は、外部から指示される他の端末に暗号化コンテンツデータを移転するための複製動作モードに応じて、配信データ解読部の動作を制御するための制御部をさらに含み、第１の記憶部は、複製動作モードが指定されるのに応じて、暗号化コンテンツデータを第２のインターフェース部に与える。

【００２０】

請求項８記載のデータ配信システムは、請求項３記載のデータ配信システムの構成に加えて、配信データ解読部は、第２の共通鍵を生成するための第３のセッションキー発生部と、第３のセッションキー発生部の出力を暗号化して第２のインターフェース部に与えることが可能な第３の暗号化処理部とをさらに含む。

【００２１】

請求項９記載のデータ配信システムは、請求項８記載のデータ配信システムの構成に加えて、第１の記憶部は、ライセンスキーに基づいて復号できる暗号化コンテンツデータをコンテンツデータ供給装置から受けて格納し、配信データ解読

部は、外部から指示される再生動作モードに応じて、第２の記憶部に格納されたライセンス情報データにより再生可能かを判断して、配信データ解読部の動作を制御するための制御部をさらに備え、第３の暗号化処理部は、第４の公開暗号化鍵により第３のセッションキー発生部の出力を暗号化して第２のインターフェース部に与え、第１の暗号化処理部は、制御部に制御されて、コンテンツデータの再生動作が指示されるのに応じて、第３の復号処理部からのライセンスキーを受けて、第３の共通鍵に基づいて暗号化して出力し、第１の記憶部は、制御部に制御されて、コンテンツデータの再生動作が指示されるのに応じて、暗号化コンテンツデータを出力し、各端末は、暗号化コンテンツデータの通信ごとに更新される第３の共通鍵を生成する第２のセッションキー発生部と、第４の公開暗号化鍵を配信データ解読部に与える公開鍵保持部と、第４の公開暗号化鍵で暗号化された第２の共通鍵を復号可能な公開鍵復号部と、配信データ解読部からの第３の共通鍵により暗号化されたライセンスキーを受けて復号して抽出し、第１の記憶部から出力された暗号化コンテンツデータをライセンスキーにより復号して再生するコンテンツデータ再生部とをさらに備える。

【００２２】

請求項１０記載のデータ配信システムは、請求項９記載のデータ配信システムの構成に加えて、配信データ解読部は、外部から指示される他の端末に暗号化コンテンツデータおよびライセンス情報データを移転するための移動動作モードに応じて、配信データ解読部の動作を制御するための制御部と、第３の公開暗号化鍵で暗号化処理を行なうための第２の暗号化処理部とをさらに含み、第２の復号処理部は、制御部に制御されて、移動動作モードが指定されるのに応じて、第３の共通鍵に基づいて暗号化されて他の端末の側から送信される第３の公開暗号化鍵を復号して抽出し、第２の暗号化処理部は、移動動作モードが指定されるのに応じて、ライセンスキーおよびライセンス情報データを第３の公開暗号化鍵で暗号化し、第１の暗号化処理部は、第２の暗号化処理部の出力を受けて、第３の共通鍵に基づいて暗号化して第２のインターフェース部に与え、制御部は、移動動作モードが指定されるのに応じて、第２の記憶部に格納されているライセンス情報データを消去し、第１の記憶部は、移動動作モードが指定されるのに応じて、

暗号化コンテンツデータを第２のインターフェース部に与える。

【００２３】

請求項１１記載のデータ配信システムは、請求項９記載のデータ配信システムの構成に加えて、配信データ解読部は、外部から指示される他の端末に暗号化コンテンツデータを移転するための複製動作モードに応じて、配信データ解読部の動作を制御するための制御部をさらに含み、第１の記憶部は、複製動作モードが指定されるのに応じて、暗号化コンテンツデータを第２のインターフェース部に与える。

【００２４】

請求項１２記載のデータ配信システムは、請求項１記載のデータ配信システムの構成に加えて、第１のインターフェース部と第２のインターフェース部とは、携帯電話網により接続され、コンテンツデータ供給装置は、第１の公開暗号鍵に基づいて、ユーザの認証を行なう。

【００２５】

請求項１３記載のデータ配信システムは、請求項１記載のデータ配信システムの構成に加えて、第１のインターフェース部は、端末と直接接続可能なコネクタ部を含む。

【００２６】

請求項１４記載のデータ配信システムは、請求項２記載のデータ配信システムの構成に加えて、第１のインターフェース部は、メモリーカードと直接接続可能な接続部を含む。

【００２７】

請求項１５記載のデータ配信システムは、コンテンツデータ供給装置から、暗号化コンテンツデータと暗号化データを復号するためのコンテンツキーとのうちの少なくとも１つを複数のユーザの各端末に配信するためのデータ配信システムであって、コンテンツデータ供給装置は、外部との間でデータを授受するための第１のインターフェイス部と、暗号化コンテンツデータの通信ごとに更新される第１の共通鍵を生成する第１のセッションキー発生部と、ユーザの端末に対応して予め定められた第１の公開暗号化鍵により第１の共通鍵を暗号化して第１のイ

ンターフェイス部に与えるためのセッションキー暗号化処理部と、第２の共通鍵により暗号化されて返信される第２の共通鍵と第２の公開暗号化鍵を復号し抽出するセッションキー復号部と、暗号化コンテンツデータを復号するためのコンテンツキーを、セッションキー復号部により復号された第２の公開暗号化鍵により暗号化するための第１のライセンスデータ暗号化処理部と、第１のライセンスデータ暗号化処理部の出力を第２の共通鍵でさらに暗号化して第１のインターフェイス部に与え配信するための第２のライセンス暗号化処理部とを備え、各端末は、外部との間でデータを授受するための第２のインターフェイス部と、暗号化コンテンツデータおよびコンテンツキーを受けて格納する配信データ解読部とを備え、配信データ解読部は、第１の公開暗号化鍵によって暗号化されたデータを復号化するための第１の秘密復号鍵を保持する第１の鍵保持部と、第１の公開暗号化鍵によって暗号化された第１の共通鍵を受けて、復号処理するための第１の復号処理部と、第２の公開暗号化鍵を保持するための第２の鍵保持部と、第２の共通鍵を生成する第２のセッションキー発生部と、第２の公開暗号化鍵と第２の共通鍵を、第１の共通鍵に基づいて暗号化し、第２のインターフェイス部に出力するための第１の暗号化処理部と、第２のライセンスデータ暗号化処理部からの暗号化されたコンテンツキーを受け、第２の共通鍵に基づいて復号するための第２の復号処理部と、第２の復号処理部の出力と、コンテンツキーにて復号可能な暗号化コンテンツデータを格納するための記憶部と、第２の公開暗号化鍵によって暗号化されたデータを復号化するための第２の秘密復号鍵を保持する第３の鍵保持部と、記憶部に格納されたデータに基づいて、第２の秘密復号鍵によりコンテンツキーを復号し抽出するための第３の復号処理部と、第１の公開暗号化鍵を少なくとも含む第１の認証データを公開認証鍵により復号できるように暗号化して保持し外部に出力可能な第１の認証データ保持部と、公開認証鍵により復号できる外部から与えられる第１の認証データを復号して抽出するための第１の認証復号処理部とを備え、コンテンツデータ供給部は、第１の認証復号処理部により抽出された第１の認証データに基づいて認証処理を行ない、少なくともコンテンツキーを配信するか否かを判断する配信制御手段をさらに含む。

【００２８】

請求項１６記載のデータ配信システムは、請求項１５記載のデータ配信システムの構成に加えて、配信データ解読部は、端末に着脱可能なメモリカードであり、第１の秘密復号鍵は、メモリカードの種類の対応して予め定められた値であり第２の秘密複号鍵は、メモリカードごとに異なる。

【００２９】

請求項１７記載のデータ配信システムは、請求項１５記載のデータ配信システムの構成に加えて、各端末は、コンテンツ再生部をさらに備え、コンテンツ再生部は、予め定められた第３の公開暗号鍵を少なくとも含む第２の認証データを公開認証鍵に基づいて復号できるように暗号化して保持し、外部に対して出力できる第２の認証データ保持部をさらに含む。

【００３０】

請求項１８記載のデータ配信システムは、請求項１７記載のデータ配信システムの構成に加えて、第１の認証復号処理部は、公開認証鍵により復号できるよう暗号化された第２の認証データをさらに復号して出力し、配信制御部は、第１の認証復号処理部にて抽出された第１の認証データおよび第２の認証データに基づいて認証処理を行ない、少なくともコンテンツキーを配信するか否かを判断する。

【００３１】

請求項１９記載のデータ配信システムは、請求項１５記載のデータ配信システムの構成に加えて、第１のインタフェイス部と第２のインタフェイス部とは、携帯電話網により接続される。

【００３２】

請求項２０記載のデータ配信システムは、請求項１５記載のデータ配信システムの構成に加えて、第１のインタフェイス部は、端末と直接接続可能なコネクタ部を含む。

【００３３】

請求項２１記載のデータ配信システムは、請求項１６記載のデータ配信システムの構成に加えて、第１のインタフェイス部は、データ格納部と直接接続可能な接続部を含む。

【００３４】

請求項２２記載のデータ配信システムは、請求項２１記載のデータ配信システムの構成に加えて、データ解読部は、接続部からのデータを受ける複数の端子を含み、外部からの指令に従って、接続部からデータを受ける端子数が切換え可能である。

【００３５】

請求項２３記載のデータ配信システムは、請求項１７記載のデータ配信システムの構成に加えて、データ再生部は、第３の公開暗号鍵にて暗号化されたデータを復号する第３の秘密復号鍵を保持するための第４の鍵保持部と、外部にて第３の公開暗号化鍵によって暗号化された第２の共通鍵を復号し抽出するための第３の復号処理部と、第３の共通鍵を生成する第３のセッションキー発生部と、第３の復号処理部にて復号し抽出した第２の共通鍵に基づいて、第３の共通鍵を暗号化し出力するための第２の暗号化処理部と、外部にて第３の共通鍵に基づいて暗号化されたコンテンツキーを復号し抽出するための第４復号処理部と、記録部に記録された暗号化コンテンツデータを抽出したコンテンツキーにて復号し、再生するためのデータ再生部とをさらに備え、配信データ解読部は、公開認証鍵により復号できるコンテンツ再生部からの与えられる暗号化された第２の認証データを復号して第３の公開鍵を抽出するための第２の認証復号処理部と、第２のセッションキー発生部にて生成した第２の共通鍵を第３の公開暗号化鍵に基づいて暗号化する第３の暗号化処理部と、データ再生部にて第２の共通鍵にて暗号化された第３の共通鍵を受けて、第１の復号処理部にて第２の共通鍵に基づいて復号した第３の共通鍵に基づいて、記録部に格納されたデータを第２の秘密復号鍵にて復号したコンテンツキーを、第１の暗号化処理部にて暗号化し、コンテンツ再生部へ出力を指示する制御部とをさらに備え、制御手段は、第２の認証復号処理部により復号された第２の認証データに基づいて認証処理を行ない、少なくともコンテンツキーを出力するか否かを判断する。

【００３６】

請求項２４記載のデータ配信システムは、請求項１６記載のデータ配信システムの構成に加えて、配信データ解読部は、第２の公開鍵によって第２の共通鍵を

暗号化するための第４の暗号化処理部をさらに含み、認証復号処理部は、外部から指示される、他の配信データ解読部に少なくともコンテンツキーを移転する移動処理に応じて、他のデータ解読部の公開認証鍵によって復号できる暗号化された第１の認証データを、公開認証鍵にて復号して、他のデータ解読部における第１の公開暗号化鍵を抽出し、第２のセッションキー発生部は、移動処理に応じて、第２の共通鍵を発生し、第３の暗号化処理部は、移動処理に応じて、他の配信データ解読部の第１の公開暗号化鍵に基づいて、第２の共通鍵を暗号化し、第２の復号処理部は、移動処理に応じて、他の配信データ解読部から第２の共通鍵によって暗号化され、入力される第４の共通鍵と他の配信データ解読部の第２の公開暗号化鍵とを復号して抽出し、第３の復号処理部は、移動処理に応じて、第２の秘密復号鍵に基づいて、記録部に格納された第２の公開暗号化鍵にて暗号化されたデータを復号し、コンテンツキーを抽出し、第４の暗号化処理部は、移動処理に応じて、他のメモリカードの第２の公開暗号化鍵に基づいて、抽出されたコンテンツキーを暗号化し、第１の暗号化処理部は、移動処理に応じて、第4の暗号化処理部の出力を第４の共通鍵にて暗号化し、他の配信データ解読部に対して出力し、制御手段は、第２の認証復号処理部により抽出された他のデータ解読部から出力された第２の認証データに基づき認証処理を行ない、少なくともコンテンツキーを出力するか否かを判断する。

【００３７】

請求項２５記載のデータ配信システムは、請求項２２記載のデータ配信システムの構成に加えて、配信データ解読部は、認証復号処理は、外部から指示される、他の配信データ解読部から少なくともコンテンツキーを移転する移動受理処理に応じて、第２の認証データ保持部が第２の認証データを出力し、第１の復号処理部は、移動受理処理に応じて、他の配信データ解読部から第１の公開暗号化鍵によって暗号化され、入力される他の配信データ解読部にて発生された第４の共通鍵を復号して抽出し、第２のセッションキー発生部は、移動受理処理に応じて、第２の共通鍵を発生し、第１の暗号化処理部は、移動受理処理に応じて、第４の共通鍵に基づいて、第２の公開暗号化鍵と第２の共通鍵とを暗号化して出力し、第２の復号処理部は、他の配信データ解読部に第２の公開暗号化鍵にて暗号化

され、さらに第２の共通鍵にて暗号化されたコンテンツキーを第２の共通鍵にて復号し、記録部に記録する。

【００３８】

請求項２６記載のデータ配信システムは、請求項２１記載のデータ配信システムの構成に加えて、コンテンツデータ供給装置は、コンテンツ再生部と共通な第５の共通鍵を保持する第５の鍵保持部と、第５の鍵保持部に保持された第５の共通鍵に基づいて、コンテンツキーを暗号化し第１のライセンス暗号化処理部に対して出力する第３のライセンス暗号化部をさらに含み、コンテンツ再生部は、第５の共通鍵を保持する第６の鍵保持手段と、第４の復号処理部とデータ再生部との間に設けられ、第６の鍵保持部に保持された第５の共通鍵によって、第４の復号処理部の出力からコンテンツキーを復号し抽出し、データ再生部に対して出力する第５の復号処理部をさらに含む。

【００３９】

請求項２７記載のデータ配信システムは、請求項２１記載のデータ配信システムの構成に加えて、コンテンツデータ供給装置は、コンテンツ再生部にて復号可能な第４の公開暗号化鍵を保持する第５の鍵保持部と、第４の公開暗号化鍵に基づいてコンテンツキーを暗号化し第１のライセンス暗号化処理部にて出力する第３のライセンス暗号化部をさらに含み、コンテンツ再生部は、第４の公開暗号化鍵によって暗号化されたデータを復号できる第４の秘密復号鍵を保持する第６の鍵保持手段と、第４の復号処理部とデータ再生部との間に設けられ、第４の秘密復号鍵によって第４の復号処理部の出力からコンテンツキーを復号し抽出し、データ再生部に対して出力する第５の復号処理部をさらに含む。

【００４０】

請求項２８記載のデータ配信システムは、請求項１６記載のデータ配信システムの構成に加えて、データ再生部は、複数の配信データ解読部を備える。

【００４１】

【発明の実施の形態】

［実施の形態１］

［システムの全体構成］

図１は、本発明の情報配信システムの全体構成を概略的に説明するための概念図である。

【００４２】

なお、以下では携帯電話網を介して、音楽データを各ユーザに配信するデータ配信システムの構成を例にとって説明するが、以下の説明で明らかとなるように、本発明はこのような場合に限定されることなく、他の著作物データ、たとえば画像データ等の著作物データを、他の情報通信網を介して配信する場合にも適用することが可能なものである。

【００４３】

図１を参照して、著作権の存在する音楽情報を管理する配信サーバ１０は、所定の暗号方式により音楽データ（以下コンテンツデータとも呼ぶ）を暗号化したうえで、情報を配信するための配信キャリア２０である携帯電話会社に、このような暗号化データを与える。一方、認証サーバ１２は、音楽データの配信を求めてアクセスしてきた機器が正規の機器であるか否かの認証を行なう。

【００４４】

配信キャリア２０は、自己の携帯電話網を通じて、各ユーザからの配信要求（配信リクエスト）を配信サーバ１０に中継する。配信サーバ１０は、配線リクエストがあると、認証サーバ１２により正規の機器からのアクセスであることを確認し、要求されたコンテンツデータをさらに暗号化したうえで、配信キャリア２０の携帯電話網を介して、各ユーザの携帯電話機に対して配信する。

【００４５】

図１においては、たとえば携帯電話ユーザ１の携帯電話機１００には、携帯電話機１００により受信された暗号化コンテンツデータを受取って、上記送信にあたって行なわれた暗号化については復号化したうえで、携帯電話機１００中の音楽再生部（図示せず）に与えるための着脱可能なメモリカード１１０に格納する構成となっている。

【００４６】

さらに、たとえばユーザ１は、携帯電話機１００に接続したヘッドホン１３０等を介してこのようなコンテンツデータを再生した音楽を聴取することが可能で

ある。

【００４７】

以下では、このような配信サーバ１０と認証サーバ１２と配信キャリア２０とを併せて、音楽サーバ３０と総称することにする。

【００４８】

また、このような音楽サーバ３０から、各携帯電話端末等にコンテンツデータを伝送する処理を「配信」と称することとする。

【００４９】

このような構成とすることで、まず、正規のメモリカードであるメモリカード１１０を購入していない正規のユーザでないものは、音楽サーバ３０からの配信データを受取って再生することが困難な構成となる。

【００５０】

しかも、配信キャリア２０において、たとえば１曲分のコンテンツデータを配信するたびにその度数を計数しておくことで、ユーザがコンテンツデータを受信（ダウンロード）するたびに発生する著作権料を、配信キャリア２０が携帯電話の通話料金として徴収することとすれば、著作権者が著作権料を確保することが容易となる。

【００５１】

しかも、このようなコンテンツデータの配信は、携帯電話網というクローズドなシステムを介して行なわれるため、インターネット等のオープンなシステムに比べて、著作権保護の対策を講じやすいという利点がある。

【００５２】

このとき、たとえばメモリカード１１２を有するユーザ２が、自己の携帯電話機１０２により、音楽サーバ３０から直接コンテンツデータの配信を受けることは可能である。しかしながら、相当量の情報量を有するコンテンツデータ等をユーザ２が直接音楽サーバ３０から受信することとすると、その受信のために比較的長い時間を要してしまう場合がある。このような場合、既に当該コンテンツデータの配信を受けているユーザ１から、そのコンテンツデータをコピーできることを可能としておけば、ユーザにとっての利便性が向上する。

【００５３】

しかしながら、著作権者の権利保護の観点からは、自由なコンテンツデータのコピーを放任することはシステム構成上許されない。

【００５４】

図１に示した例では、ユーザ１が受信したコンテンツデータを、コンテンツデータそのものおよび当該コンテンツデータを再生可能とするために必要な情報とともに、ユーザ２に対してコピーさせる場合をコンテンツデータの「移動」と呼ぶ。この場合、ユーザ１は、再生のために必要な情報（再生情報）ごとユーザ２にコピーさせるため、情報の移動を行なった後には、ユーザ１においてはコンテンツデータの再生を行なうことは不可能とする必要がある。ここで、コンテンツデータは所定の暗号化方式にしたがって暗号化された暗号化コンテンツデータとして配信され、「再生情報」とは、後に説明するように、上記所定の暗号化方式にしたがって暗号化コンテンツデータを復号可能なライセンスキーとも称する）と、著作権保護に関わる情報であるライセンスＩＤデータやユーザＩＤデータ等のライセンス情報とを意味する。

【００５５】

これに対して、コンテンツデータのみを暗号化されたままの状態で、ユーザ２にコピーさせることを音楽情報の「複製」と呼ぶこととする。

【００５６】

この場合、ユーザ２の端末には、このようなコンテンツデータを再生させるために必要な再生情報はコピーされないので、ユーザ２は、暗号化コンテンツデータを得ただけでは、音楽を再生させることができない。したがって、ユーザ２が、このような音楽の再生を望む場合は、改めて音楽サーバ３０からコンテンツデータの再生を可能とするための再生情報の配信を受ける必要がある。しかしながら、この場合は、再生を可能とするための情報の配信のみを受ければよいため、ユーザ２が直接音楽サーバ３０からすべての配信を受ける場合に比べて、格段に短い通話時間で、音楽再生を可能とすることができる。

【００５７】

たとえば、携帯電話機１００および１０２が、ＰＨＳ（Personal Handy Phone

）である場合には、いわゆるトランシーバモードの通話が可能となっているので、このような機能を利用して、ユーザ１からユーザ２への一括した情報の移転（移動）や、暗号化したコンテンツデータのみの転送（複製）を行なうことが可能である。

【００５８】

図１に示したような構成においては、暗号化して配信されるコンテンツデータをユーザ側で再生可能とするためにシステム上必要とされるのは、第１には、通信における暗号化キー（鍵）を配送するための方式であり、さらに第２には、配信データを暗号化する方式そのものであり、さらに、第３には、このようにして配信されたデータの無断コピーを防止するためのデータ保護を実現する構成である。

【００５９】

［暗号／復号鍵の構成］

図２は、図１に示した情報配信システムにおいて使用される通信のためのキーデータ（鍵データ）等の特性をまとめて説明するための図である。

【００６０】

まず、図１に示した構成において、メモリカード１００内のデータ処理を管理するための鍵としては、メモリカードという媒体の種類に固有であり、かつ、メモリカードの種類等を個別に特定するための情報を含む秘密復号鍵Ｋｍｅｄｉａ（ｎ）（ｎ：自然数）と、メモリカードごとに異なる公開暗号化鍵ＫＰｃａｒｄ（ｎ）と、公開暗号化鍵ＫＰｃａｒｄ（ｎ）により暗号化されたデータを復号するための秘密復号鍵Ｋｃａｒｄ（ｎ）とがある。

【００６１】

ここで、鍵Ｋｃａｒｄ（ｎ）や鍵ＫＰｃａｒｄ（ｎ）の表記中の自然数ｎは、各メモリカードを区別するための番号を表わす。

【００６２】

すなわち、公開暗号化鍵ＫＰｃａｒｄ（ｎ）で暗号化されたデータは、各メモリカードごとに存在する秘密復号鍵Ｋｃａｒｄ（ｎ）で復号可能である。したがって、メモリカードにおける配信データの授受にあたっては、基本的には、後に

説明するように３つの暗号鍵Ｋｍｅｄｉａ（ｎ）、Ｋｃａｒｄ（ｎ）、ＫＰｃａｒｄ（ｎ）が用いられることになる。

【００６３】

さらに、メモリカード外とメモリカード間でのデータの授受における秘密保持のための暗号鍵としては、各媒体に固有な公開暗号化鍵ＫＰｍｅｄｉａ（ｎ）と、公開暗号化鍵ＫＰｍｅｄｉａ（ｎ）により暗号化されたデータを復号化するための秘密復号鍵Ｋｍｅｄｉａ（ｎ）と、各通信ごと、たとえば、音楽サーバ３０へのユーザのアクセスごとに音楽サーバ３０、携帯電話機１００または１０２において生成される共通鍵Ｋｓが用いられる。

【００６４】

ここで、共通鍵Ｋｓは、たとえば、ユーザが音楽サーバ３０に対して１回のアクセスを行なうごとに発生する構成として、１回のアクセスである限り何曲の音楽情報についても同一の共通鍵が用いられる構成としてもよいし、また、たとえば、各曲目ごとにこの共通鍵を変更したうえでその都度ユーザに配信する構成としてもよい。

【００６５】

以下では、このような通信の単位あるいはアクセスの単位を「セッション」と呼ぶことにし、共通鍵Ｋｓを「セッションキー」とも呼ぶことにする。

【００６６】

したがって、共通鍵Ｋｓは各通信セッションに固有の値を有することになり、配信サーバや携帯電話機において管理される。

【００６７】

また、配信されるべきデータについては、まず、暗号化コンテンツデータを復号する鍵であるＫｃ（以下、ライセンスキーと呼ぶ）があり、このライセンスキーＫｃにより暗号化コンテンツデータが復号化されるものとする。さらに、上述したライセンス情報として、当該コンテンツデータを特定できる管理コードや、再生を行なう回数の制限などの情報を含むライセンスＩＤデータＬｉｃｅｎｓｅ－ＩＤ等が存在する。一方、携帯電話は、受信者を識別するためのユーザＩＤデータＵｓｅｒ－ＩＤを保持している。

【００６８】

このような構成とすることで、ライセンスＩＤデータに含まれる情報に応じて、著作権者側の著作権保護に関する制御を行なうことが可能であり、一方ユーザＩＤデータを用いることで、ユーザの個人情報の保護、たとえばユーザのアクセス履歴等が部外者から知ることができないように保護するといったような制御を行なうことが可能である。

【００６９】

配信データにおけるコンテンツデータＤｃは、上述のとおり、たとえば音楽データであり、このコンテンツデータをライセンスキーＫｃで復号化可能なデータを、暗号化コンテンツデータ［Ｄｃ］Ｋｃと呼ぶ。

【００７０】

ここで、［Ｙ］Ｘという表記は、データＹを、キー（鍵）Ｘにより復号可能な暗号に変換したデータであることを示している。なお、暗号化処理、復号処理で用いられる鍵を、「キー」とも称することとする。

【００７１】

［配信サーバ１０の構成］

図３は、図１に示した配信サーバ１０の構成を示す概略ブロック図である。配信サーバ１０は、コンテンツデータ（音楽データ）を所定の方式に従って暗号化したデータや、ライセンスＩＤ等の配信情報を保持するための配信情報データベース３０４と、各ユーザごとにコンテンツデータへのアクセス回数等に従った課金情報を保持するための課金データベース３０２と、配信情報データベース３０４および課金データベース３０２からのデータをデータバスＢＳ１を介して受取り、所定の暗号化処理を行なうためのデータ処理部３１０と、通信網を介して、配信キャリア２０とデータ処理部３１０との間でデータ授受を行なうための通信装置３５０とを備える。

【００７２】

データ処理部３１０は、データバスＢＳ１上のデータに応じて、データ処理部３１０の動作を制御するための配信制御部３１２と、配信制御部３１２に制御されて、セッションキーＫｓを発生するためのセッションキー発生部３１４と、セ

ッションキー発生部３１４より生成されたセッションキーＫｓを、公開暗号化鍵ＫＰｍｅｄｉａにより暗号化して、データバスＢＳ１に与えるための暗号化処理部３１６と、各ユーザの携帯電話機においてセッションキーＫｓにより暗号化されたうえで送信されたデータを通信装置３５０およびデータバスＢＳ１を介して受けて、復号処理を行なう復号処理部３１８と、復号処理部３１８により抽出された公開暗号化鍵ＫＰｃａｒｄ（ｎ）を用いて、ライセンスキーやライセンスＩＤ等のデータを配信制御部３１２に制御されて暗号化するための暗号化処理部３２０と、暗号化処理部３２０の出力を、さらにセッションキーＫｓにより暗号化して、データバスＢＳ１を介して通信装置３５０に与える暗号化処理部３２２とを含む。

【００７３】

［端末（携帯電話機）の構成］

図４は、図１に示した携帯電話機１００の構成を説明するための概略ブロック図である。

【００７４】

携帯電話機１００は、携帯電話網により無線伝送される信号を受信するためのアンテナ１１０２と、アンテナ１１０２からの信号を受けてベースバンド信号に変換し、あるいは携帯電話機からのデータを変調してアンテナ１１０２に与えるための送受信部１１０４と、携帯電話機１００の各部のデータ授受を行なうためのデータバスＢＳ２と、データバスＢＳ２を介して携帯電話機１００の動作を制御するためのコントローラ１１０６と、受信者を識別するためのユーザＩＤデータＵｓｅｒ－ＩＤを保持するユーザＩＤ保持部１１０７と、外部からの指示を携帯電話機１００に与えるためのタッチキー部１１０８と、コントローラ１１０６等から出力される情報をユーザに視覚情報として与えるためのディスプレイ１１１０と、通常の通話動作において、データバスＢＳ２を介して与えられる受信データに基づいて音声を再生するための音声再生部１１１２と、外部との間でデータの授受を行なうためのコネクタ１１２０と、コネクタ１１２０からのデータをデータバスＢＳ２に与え得る信号に変換し、または、データバスＢＳ２からのデータをコネクタ１１２０に与え得る信号に変換するための外部インターフェース

部１１２２とを備える。

【００７５】

ここで、ユーザＩＤデータは、たとえばユーザの電話番号等のデータを含む。

携帯電話機１００は、さらに、音楽サーバ３０からのコンテンツデータを復号化処理するための着脱可能なメモリカード１１０と、メモリカード１１０とデータバスＢＳ２との間のデータの授受を制御するためのメモリインタフェース１２００と、メモリカード１１０と携帯電話機の他の部分とのデータ授受にあたり、データバスＢＳ２上においてやり取りされるデータを暗号化するためのセッションキーＫｓを乱数等により発生するセッションキー発生部１５０２と、セッションキー発生部１５０２により生成されたセッションキーを暗号化して、データバスＢＳ２に与えるための暗号化処理部１５０４と、セッションキー発生部１５０２において生成された、データバスＢＳ２上のデータをセッションキーＫｓにより復号して出力する復号処理部１５０６と、復号処理部１５０６の出力を受けて、音楽信号を再生するための音楽再生部１５０８と、音楽再生部１５０８の出力と音声再生部１１１２の出力とを受けて、動作モードに応じて選択的に出力するための混合部１５１０と、混合部１５１０の出力を受けて、外部に出力するためのアナログ信号に変換するデジタルアナログ変換部１５１２と、デジタルアナログ変換部１５１２の出力を受けて、ヘッドホン１３０と接続するための接続端子１５１４とを含む。

【００７６】

なお、説明の簡素化のため本発明のコンテンツデータの配信に関わるブロックのみを記載し、携帯電話機が本来備えている通話機能に関するブロックについては、一部割愛されている。

【００７７】

［メモリカードの構成］

図５は、図４に示したメモリカード１１０の構成を説明するための概略ブロック図である。

【００７８】

以下では、端末１００に装着されるメモリカード１１０の公開暗号化鍵ＫＰｍ

ｅｄｉａと、端末１０２に装着されるメモリカード１１２の公開暗号化鍵ＫＰｍｅｄｉａとを区別して、それぞれ、メモリカード１１０に対するものを公開暗号化鍵ＫＰｍｅｄｉａ（１）と、メモリカード１１２に対するものを公開暗号化鍵ＫＰｍｅｄｉａ（２）と称することにする。

【００７９】

また、これに対応して、公開暗号化鍵ＫＰｍｅｄｉａ（１）で暗号化されたデータを復号可能であって、これとは非対称な秘密復号鍵を秘密復号鍵Ｋｍｅｄｉａ（１）と称し、公開暗号化鍵ＫＰｍｅｄｉａ（２）で暗号化されたデータを復号可能であって、これとは非対称な秘密復号鍵を秘密復号鍵Ｋｍｅｄｉａ（２）と称することにする。

【００８０】

このように、媒体固有の公開暗号化鍵を区別することにより、以下の説明で明らかとなるように、メモリカードに複数の種類が存在する場合や、より一般的に、メモリカード以外の媒体がシステムのオプションとして存在する場合にも、対応することが可能となる。

【００８１】

メモリカード１１０は、メモリインタフェース１２００との間で信号を端子１２０２を介して授受するデータバスＢＳ３と、公開暗号化鍵ＫＰｍｅｄｉａ（１）の値を保持し、データバスＢＳ３に公開暗号化鍵ＫＰｍｅｄｉａ（１）を出力するためのＫＰｍｅｄｉａ（１）保持部１４０１と、メモリカード１１０に対応する秘密復号鍵Ｋｍｅｄｉａ（１）を保持するためのＫｍｅｄｉａ（１）保持部１４０２と、データバスＢＳ３にメモリインタフェース１２００から与えられるデータから、秘密復号鍵Ｋｍｅｄｉａ（１）により復号処理をすることにより、セッションキーＫｓを抽出する復号処理部１４０４と、公開暗号化鍵ＫＰｃａｒｄ（１）を保持するためのＫＰｃａｒｄ（１）保持部１４０５と、復号処理部１４０４により抽出されたセッションキーＫｓに基づいて、切換スイッチ１４０８からの出力を暗号化してデータバスＢＳ３に与えるための暗号化処理部１４０６と、データバスＢＳ３上のデータを復号処理部１４０４により抽出されたセッションキーＫｓにより復号処理してデータバスＢＳ４に与えるための復号処理部１

４１０と、データバスＢＳ４からメモリカードごとに異なる公開暗号化鍵ＫＰｃａｒｄ（ｎ）で暗号化されているライセンスキーＫｃ、ライセンスＩＤ等のデータを格納し、データバスＢＳ３からライセンスキーＫｃにより暗号化されている暗号化コンテンツデータ［Ｄｃ］Ｋｃを受けて格納するためのメモリ１４１２とを備える。

【００８２】

切換えスイッチ１４０８は、接点Ｐａ、Ｐｂ、Ｐｃを有し、接点ＰａにはＫＰｃａｒｄ（１）保持部１４０５からの公開暗号化鍵ＫＰｃａｒｄ（１）が，接点ＰｂにはデータバスＢＳ５が、接点Ｐｃには暗号化処理部１４１４の出力が与えられる。切換えスイッチ１４０８は、それぞれ、接点Ｐａ、Ｐｂ、Ｐｃに与えられる信号を、動作モードが、「配信モード」、「再生モード」、「移動モード」のいずれであるかに応じて、選択的に暗号化処理部１４０６に与える。

【００８３】

メモリカード１１０は、さらに、秘密復号鍵Ｋｃａｒｄ（１）の値を保持するためのＫｃａｒｄ（１）保持部１４１５と、公開暗号化鍵ＫＰｃａｒｄ（１）により暗号化されており、かつ、メモリ１４１２から読み出されたライセンスキーＫｃ、ライセンスＩＤ等（［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１））を、復号処理してデータバスＢＳ５に与える復号処理部１４１６と、データの移動処理等において、相手先のメモリカードの公開暗号化鍵ＫＰｃａｒｄ（ｎ）を復号処理部１４１０から受けて、この相手方の公開暗号化鍵ＫＰｃａｒｄ（ｎ）に基づいて、データバスＢＳ５上に出力されているライセンスキーＫｃ、ライセンスＩＤ等を暗号化したうえで、切換スイッチ１４０８に出力するための暗号化処理部１４１４と、データバスＢＳ３を介して外部とデータの授受を行い、データバスＢＳ５との間でライセンスＩＤデータ等を受けて、メモリカード１１０の動作を制御するためのコントローラ１４２０と、データバスＢＳ５との間でライセンスＩＤデータ等のデータの授受が可能なレジスタ１５００とを備える。

【００８４】

なお、図５において実線で囲んだ領域は、メモリカード１１０内において、外部からの不当な開封処理等が行なわれると、内部データの消去や内部回路の破壊

により、第三者に対してその領域内に存在する回路内のデータ等の読み出しを不能化するためのモジュールＴＲＭに組込まれているものとする。

【００８５】

このようなモジュールは、一般にはタンパーレジスタンスモジュール（Tamper Resistance Module）と呼ばれる。

【００８６】

もちろん、メモリ１４１２も含めて、モジュールＴＲＭ内に組み込まれる構成としてもよい。しかしながら、図５に示したような構成とすることで、メモリ１４１２中に保持されているデータは、いずれも暗号化されているデータであるため、第三者はこのメモリ１４１２中のデータのみでは、音楽を再生することは不可能であり、かつ高価なタンパーレジスタンスモジュール内にメモリ１４１２を設ける必要がないので、製造コストが低減されるという利点がある。

【００８７】

図６および図７は、図１および図３～図５で説明したデータ配信システムにおける配信動作を説明するための第１および第２のフローチャートである。

【００８８】

図６および図７においては、ユーザ１が、メモリカード１１０を用いることで、音楽サーバ３０から音楽データの配信を受ける場合の動作を説明している。

【００８９】

まず、ユーザ１の携帯電話機１００から、ユーザによりタッチキー１１０８のキーボタンの操作等によって、配信リクエストがなされる（ステップＳ１００）。

【００９０】

メモリカード１１０においては、この配信リクエストに応じて、ＫＰｍｅｄｉａ（１）保持部１４０１から、公開暗号化鍵ＫＰｍｅｄｉａ（１）を音楽サーバ３０に対して送信する（ステップＳ１０２）。

【００９１】

音楽サーバ３０では、メモリカード１１０から転送された配信リクエストならびに公開暗号化鍵ＫＰｍｅｄｉａ（１）を受信すると（ステップＳ１０４）、受

信した公開暗号化鍵ＫＰｍｅｄｉａ（１）に基づいて、認証サーバ１２に対して照会を行ない、正規メモリカードからのアクセスの場合は次の処理に移行し（ステップＳ１０６）、正規メモリカードでない場合には、処理を終了する（ステップＳ１５４）。

【００９２】

照会の結果、正規メモリカードであることが確認されると、音楽サーバ３０では、セッションキー発生部３１４が、セッションキーＫｓを生成する。さらに、音楽サーバ３０内の暗号化処理部３１６が、受信した公開暗号化鍵ＫＰｍｅｄｉａ（１）により、このセッションキーＫｓを暗号化して暗号化セッションキー［Ｋｓ］Ｋｍｅｄｉａ（１）を生成する（ステップＳ１０８）。

【００９３】

続いて、音楽サーバ３０は、暗号化セッションキー［Ｋｓ］Ｋｍｅｄｉａ（１）をデータバスＢＳ１に与える。通信装置３５０は、暗号化処理部３１６からの暗号化セッションキー［Ｋｓ］Ｋｍｅｄｉａ（１）を、通信網を通じて、携帯電話機１００のメモリカード１１０に対して送信する（ステップＳ１１０）。

【００９４】

携帯電話機１００が、暗号化セッションキー［Ｋｓ］Ｋｍｅｄｉａ（１）を受信すると（ステップＳ１１２）、メモリカード１１０においては、メモリインタフェース１２００を介して、データバスＢＳ３に与えられた受信データを、復号処理部１４０４が、秘密復号鍵Ｋｍｅｄｉａ（１）により復号処理することにより、セッションキーＫｓを復号し抽出する（ステップＳ１１４）。

【００９５】

続いて、配信動作においては、切換スイッチ１４０８は、接点Ｐａが閉じる状態が選択されているので、暗号化処理部１４０６は、接点Ｐａを介してＫＰｃａｒｄ（１）保持部１４０５から与えられる公開暗号化鍵ＫＰｃａｒｄ（１）（メモリカード１１０に対する公開暗号化鍵）を、セッションキーＫｓにより暗号化し（ステップＳ１１６）、データ［ＫＰｃａｒｄ（１）］Ｋｓを生成する（ステップＳ１１８）。

【００９６】

携帯電話機１００は、暗号化処理部１４０６により暗号化されたデータ［ＫＰｃａｒｄ（１）］Ｋｓを音楽サーバ３０に対して送信する（ステップＳ１２０）。

【００９７】

音楽サーバ３０では、通信装置３５０によりデータ［ＫＰｃａｒｄ（１）］Ｋｓが受信され（ステップＳ１２２）、データバスＢＳ１に与えられたデータ［ＫＰｃａｒｄ（１）］Ｋｓを復号処理部３１８が、セッションキーＫｓにより復号処理して、公開暗号化鍵ＫＰｃａｒｄ（１）を復号抽出する（ステップＳ１２４）。

【００９８】

続いて、配信制御部３１２は、配信情報データベース３０４等に保持されているデータを元に、ライセンスＩＤデータ等を含むライセンス情報データＬｉｃｅｎｓｅを生成する（ステップＳ１２６）。

【００９９】

さらに、音楽サーバ３０は、暗号化コンテンツデータ［Ｄｃ］Ｋｃを配信情報データベース３０４より取得して、通信装置３５０を介して、メモリカード１１０に送信する（ステップＳ１２８）。

【０１００】

携帯電話機１００がデータ［Ｄｃ］Ｋｃを受信すると（ステップＳ１３０）、メモリカード１１０においては、受信したデータ［Ｄｃ］Ｋｃをそのままメモリ１４１２に格納する（ステップＳ１３２）。

【０１０１】

一方、音楽サーバ３０は、ライセンスキーＫｃを配信情報データベース３０４より取得し（ステップＳ１３４）、暗号化処理部３２０は、配信制御部３１２からのライセンスキーＫｃとライセンス情報データＬｉｃｅｎｓｅとを、復号処理部３１８より与えられた公開暗号化鍵ＫＰｃａｒｄ（１）により暗号化処理する（ステップＳ１３６）。

【０１０２】

暗号化処理部３２２は、暗号化処理部３２０により暗号化されたデータ［Ｋｃ

、Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）を受取って、さらにセッションキーＫｓにより暗号化したデータをデータバスＢＳ１に与える。通信装置３５０は、暗号化処理部３２２により暗号化されたデータ［［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）］Ｋｓをメモリカード１１０に対して送信する。

【０１０３】

携帯電話機１００がデータ［［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）］Ｋｓを受信すると（ステップＳ１４２）、メモリカード１１０においては、復号処理部１４１０がセッションキーＫｓにより復号処理を行ない、データ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）を抽出し、メモリ１４１２に記録（格納）する（ステップＳ１４６）。

【０１０４】

さらに、メモリカード１１０においては、コントローラ１４２０により制御されて、復号処理部１４１６が、メモリ１４１２に格納されたデータ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）を復号し、復号されたライセンス情報データＬｉｃｅｎｓｅを、レジスタ１５００に格納する（ステップ１４８）。

【０１０５】

以上のような動作により、メモリカード自身が、セッションキーＫｓを送る側（音楽サーバ３０）に、公開暗号化鍵ＫＰｍｅｄｉａ（１）を送信した上で、配信を受けることができ、メモリカード１１０が格納するコンテンツデータは再生可能な状態となる。以下では、メモリカードが格納するコンテンツデータが再生可能な状態となっていることを、「メモリカード１１０は、状態ＳＡにある」と呼ぶことにする。一方、メモリカードが格納するコンテンツデータが再生不可能な状態となっていることを、「メモリカード１１０は、状態ＳＢにある」と呼ぶことにする。

【０１０６】

さらに、メモリカード１１０から音楽サーバ３０へは、配信受理が通知され、音楽サーバ３０で配信受理を受信すると（ステップＳ１５０）、課金データベース３０２にユーザ１の課金データが格納され（ステップＳ１５２）、処理が終了する（ステップＳ１５４）。

【０１０７】

図８は、携帯電話機１００内において、メモリカード１１０に保持された暗号化コンテンツデータから、コンテンツデータを復号化し、音楽として外部に出力するための再生処理を説明するフローチャートである。

【０１０８】

図８を参照して、携帯電話機１００のタッチキー部１１０８等からのユーザ１の指示により、再生リクエストがメモリカード１１０に対して出力される（ステップＳ２００）。

【０１０９】

メモリカード１１０においては、この再生リクエストに応じて、コントローラ１４２０は、レジスタ１５００に保持されるライセンス情報データＬｉｃｅｎｓｅに基づいて、再生可能なデータに対するリクエストであるかを判断し（ステップＳ２０２）、再生可能と判断した場合は、ＫＰｍｅｄｉａ（１）保持部１４０１から、公開暗号化鍵ＫＰｍｅｄｉａ（１）を携帯電話機１００に対して送信する（ステップＳ２０４）。一方、再生不可能と判断した場合は、処理を終了する（ステップＳ２３０）。

【０１１０】

再生可能と判断され、メモリカード１１０から公開暗号化鍵ＫＰｍｅｄｉａ（１）が送信された場合、携帯電話機１００では、メモリカード１１０からの公開暗号化鍵ＫＰｍｅｄｉａ（１）を受信すると（ステップＳ２０６）、Ｋｓ発生部１５０２においてセッションキーＫｓを生成し、暗号化処理部１５０４が、公開暗号化鍵ＫＰｍｅｄｉａ（１）により、セッションキーＫｓを暗号化して暗号化セッションキー［Ｋｓ］ＫＰｍｅｄｉａ（１）を生成し、データバスＢＳ２を介して、メモリカード１１０に対して送信する（ステップＳ２０８）。

【０１１１】

メモリカード１１０は、データバスＢＳ２を介して、携帯電話機１００により生成され、かつ暗号化されたセッションキーＫｓを受け取り、秘密復号鍵Ｋｍｅｄｉａ（１）により復号し、セッションキーＫｓを抽出する（ステップＳ２１０）。

【０１１２】

続いて、メモリカード１１０は、メモリ１４１２から、暗号化されているデータ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）を読み出し、復号処理部１４１６が復号処理を行なう（ステップＳ２１２）。

【０１１３】

秘密復号鍵Ｋｃａｒｄ（１）により、メモリ１４１２から読み出されたデータを復号可能な場合（ステップＳ２１４）、ライセンスキーＫｃが抽出される（ステップＳ２１６）。　一方、再生不可能の場合、処理は終了する（ステップＳ２３２）。

【０１１４】

メモリ１４１２から読み出されたデータを再生可能な場合（ステップＳ２１４）は、レジスタ１５００内のライセンス情報データＬｉｃｅｎｓｅのうち、再生回数に関するデータが変更される（ステップＳ２１８）。

【０１１５】

続いて、抽出したセッションキーＫｓにより、ライセンスキーＫｃを暗号化し（ステップＳ２２０）、暗号化されたライセンスキー［Ｋｃ］Ｋｓをデータバス ＢＳ２に与える（ステップＳ２２２）。

【０１１６】

携帯電話機１００の復号処理部１５０６は、セッションキーＫｓにより復号化処理を行なうことにより、ライセンスキーＫｃを取得する（ステップＳ２２４）。

【０１１７】

続いて、メモリカード１１０は、暗号化コンテンツデータ［Ｄｃ］Ｋｃをメモリ１４１２から読み出し、データバスＢＳ２に与える（ステップＳ２２６）。

【０１１８】

携帯電話機１００の音楽再生部１５０８は、暗号化コンテンツデータ［Ｄｃ］Ｋｃを、抽出されたライセンスキーＫｃにより復号処理して平文の音楽データを生成し（ステップＳ２２８）、音楽信号を再生して混合部１５１０に与える（ステップＳ２３０）。デジタルアナログ変換部１５１２は、混合部１５１０からの

データを受け取って変換し、外部に再生された音楽を出力し、処理が終了する（ステップＳ２３２）。

【０１１９】

このような構成とすることで、メモリカード自身が、セッションキーＫｓを送る側（携帯電話機１００）に、公開暗号化鍵ＫＰｍｅｄｉａ（１）を送信した上で、再生動作を行なうことが可能となる。

【０１２０】

図９および図１０は、２つのメモリカード間において、音楽データおよびキーデータ等の移動または複製を行なう処理を説明するための第１および第２のフローチャートである。

【０１２１】

まず、携帯電話機１０２が送信側であり、携帯電話機１００が受信側であるものとする。また、携帯電話機１０２にも、メモリカード１１０と同様の構成を有するメモリカード１１２が装着されているものとする。

【０１２２】

携帯電話機１０２は、まず、自身の側のメモリカード１１２および携帯電話機１００に対して、移動リクエストまたは複製リクエストを出力する（ステップＳ３００）。

【０１２３】

メモリカード１１２は、これに応じて、メモリ１４１２内の暗号化コンテンツデータ［Ｄｃ］Ｋｃを読み出して、メモリカード１１０に対して出力し（ステップＳ３０２）、一方、携帯電話機１００は、携帯電話機１０２からリクエストを受信して（ステップＳ３０１）、メモリカード１１０では、暗号化コンテンツデータ［Ｄｃ］ＫｃをメモリＩ４１２に格納する（ステップＳ３０４）。

【０１２４】

続いて、携帯電話機１０２および１００においては、ステップＳ３００において与えられたリクエストが、「移動リクエスト」であるか「複製リクエスト」であるかが判断され（ステップＳ３０６、ステップＳ３０６′）、「移動リクエスト」である場合、メモリカード１１２は、公開暗号化鍵ＫＰｍｅｄｉａ（２）を

携帯電話機１０２に対して送信し（ステップＳ３０８）、携帯電話機１０２は、公開暗号化鍵ＫＰｍｅｄｉａ（２）を受信する（ステップＳ３１２）。一方、メモリカード１１０は、「移動リクエスト」である場合、公開暗号化鍵ＫＰｍｅｄｉａ（１）を携帯電話機１００に出力し（ステップＳ３０８′）、携帯電話機１００は、公開暗号化鍵ＫＰｍｅｄｉａ（１）を携帯電話機１０２に対して送信する（ステップＳ３１０）。

【０１２５】

携帯電話機１０２が、公開暗号化鍵ＫＰｍｅｄｉａ（１）および公開暗号化鍵ＫＰｍｅｄｉａ（２）を受信すると（ステップＳ３１２、ステップＳ３１２′）、携帯電話機１０２においては、セッションキー発生回路１５０２は、セッションキーＫｓを生成し（ステップＳ３０３）、公開暗号化鍵ＫＰｍｅｄｉａ（１）および公開暗号化鍵ＫＰｍｅｄｉａ（２）を用いて、暗号化処理部１５０４がセッションキーＫｓを暗号化する（ステップＳ３１４）。

【０１２６】

携帯電話機１０２は、データバスＢＳ２を介して、メモリカード１１２に対しては暗号化セッションキー［Ｋｓ］ＫＰｍｅｄｉａ（２）を伝達し、メモリカード１１２においては、秘密復号鍵Ｋｍｅｄｉａ（２）によりセッションキーＫｓを復号抽出する（ステップＳ３２８）。

【０１２７】

さらに、携帯電話機１０２は、暗号化セッションキー［Ｋｓ］ＫＰｍｅｄｉａ（１）を携帯電話機１００に対して送信する（ステップＳ３１６）。携帯電話機１００は、暗号化セッションキー［Ｋｓ］ＫＰｍｅｄｉａ（１）を受信すると（ステップＳ３１８）、メモリカード１１０に伝達し、メモリカード１１０は、復号処理部１４０４が復号して、セッションキーＫｓを受理する（ステップＳ３２０）。

【０１２８】

メモリカード１１０においては、セッションキーＫｓによりメモリカード１１０の公開暗号化鍵ＫＰｃａｒｄ（１）を暗号化して（ステップＳ３２２）、携帯電話機１００から携帯電話機１０２に対して暗号化されたデータ［ＫＰｃａｒｄ

（１）］Ｋｓを送信する（ステップＳ３２４）。携帯電話機１０２は、データ［ＫＰｃａｒｄ（１）］Ｋｓを受信し（ステップＳ３２６）、かつ、メモリカード１１２によるセッションキーＫｓの受理が完了すると（ステップＳ３２８）、メモリカード１１２においては、メモリカード１１０から送信された暗号化データ［ＫＰｃａｒｄ（１）］Ｋｓをセッションキーによりメモリカード１１０の公開暗号化鍵ＫＰｃａｒｄ（１）を復号抽出する（ステップＳ３３０）。

【０１２９】

続いて、メモリカード１１２においては、メモリ１４１２からメモリカード１１２の公開暗号化鍵ＫＰｃａｒｄ（２）により暗号化されているライセンスキーＫｃ、ライセンス情報データＬｉｃｅｎｓｅが読み出される（ステップＳ３３２）。

【０１３０】

続いて、メモリカード１１２の復号処理部１４１６が、秘密復号鍵Ｋｃａｒｄ（２）により、ライセンスキーＫｃ、ライセンス情報データＬｉｃｅｎｓｅを復号処理する（ステップＳ３３４）。

【０１３１】

メモリカード１１２のコントローラ１４２０は、このようにして復号されたライセンス情報データＬｉｃｅｎｓｅの値を、レジスタ１５００内のデータ値と置換する（ステップＳ３３６）。

【０１３２】

さらに、メモリカード１１２の暗号化処理部１４１４は、復号処理部１４１０において抽出されたメモリカード１１０における公開暗号化鍵ＫＰｃａｒｄ（１）により、ライセンスキーＫｃ、ライセンス情報データＬｉｃｅｎｓｅとを暗号化する（ステップＳ３３８）。

【０１３３】

メモリカード１１２の暗号化処理部１４１４により暗号化されたデータは、切換スイッチ１４０８（接点Ｐｃが閉じている）を介して、さらに、暗号化処理部１４０６に与えられ、暗号化処理部１４０６は、データ［Ｋｃ，Ｌｉｃｅｎｓｅ

］Ｋｃａｒｄ（１）をセッションキーＫｓにより暗号化してデータ［［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）］Ｋｓを生成する（ステップＳ３４０）。

【０１３４】

続いて、メモリカード１１２は、携帯電話機１０２に対してデータ［［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）］Ｋｓを出力し（ステップＳ３４２）、携帯電話機１０２はデータ［［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）］Ｋｓを携帯電話機１００に対して送信する（ステップＳ３４４）。

【０１３５】

携帯電話機１００が受信したデータ［［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）］Ｋｓは（ステップＳ３４６）、メモリカード１１０に対して伝達され、メモリカード１１０の復号処理部１４１０は、暗号化されたデータ［［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）］Ｋｓを復号して、データ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）を受理する（ステップＳ３４８）。

【０１３６】

メモリカード１１０においては、復号処理部１４１０により、セッションキーＫｓに基づいて復号化処理されたデータをメモリ１４１２に記録する（ステップＳ３５０）。さらに、メモリカード１１０においては、復号処理部１４１６が、秘密復号鍵Ｋｃａｒｄ（１）に基づいて、データ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）を復号し、復号されたライセンス情報データＬｉｃｅｎｓｅをレジスタ１５００に格納する（ステップＳ３５２）。

【０１３７】

復号されたライセンス情報データＬｉｃｅｎｓｅのレジスタ１５００への格納が終了すると、メモリカード１１０は携帯電話機１００に移動受理を通知し、携帯電話機１００は、携帯電話機１０２に対して移動受理を送信する（ステップＳ３５４）。

【０１３８】

携帯電話機１０２は、携帯電話機１００からの移動受理を受信すると、メモリカード１１２に対してこれを転送し、メモリカード１１２は、これに応じて、レジスタ１５００に格納されたライセンス情報データＬｉｃｅｎｓｅを消去する（

ステップ３５８）。

【０１３９】

一方、携帯電話機１０２では、移動受理が受信されたことに応じて、ディスプレイ１１１０上に、ユーザ２に対して、メモリカード１１２のメモリ１４１２内に格納されている移動データに対応する記憶データの消去を行なって良いかを問うメッセージを表示する。これに応じて、ユーザ２は、タッチキー１１０８からこのメッセージに対する回答を入力する（ステップＳ３６０）。

【０１４０】

レジスタ１５００内のデータの消去が完了し（ステップＳ３５８）、かつ、上記メッセージに対する回答の入力が行なわれると（ステップＳ３６０）、メモリカード１１２内のコントローラ１４２０は、メモリ１４１２内のデータの消去を行なうかの判断を行なう（ステップＳ３６２）。

【０１４１】

メモリ１４１２内の該当データの消去が指示されている場合（ステップＳ３６２）、コントローラ１４２０により制御されて、メモリ１４１２内の暗号化コンテンツデータ［Ｄｃ］Ｋｃおよびデータ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（２）が消去され（ステップＳ３６４）、処理が終了する（ステップＳ３７４）。

【０１４２】

一方、メモリ１４１２内の該当データの消去が指示されていない場合（ステップＳ３６２）、処理は終了する（ステップＳ３７４）。この場合、メモリ１４１２内には、暗号化コンテンツデータ［Ｄｃ］Ｋｃおよびデータ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（２）が残っていることになるが、レジスタ１５００内にライセンス情報データＬｉｃｅｎｓｅが存在しないため、ユーザ２は、再度、音楽サーバ３０から再生情報を配信してもらわない限り、音楽データの再生を行なうことはできない。すなわち、メモリカード１１２は「状態ＳＢ」となる。メモリカード１１０においては、暗号化コンテンツデータ以外にも、ライセンスキーＫｃ、ライセンス情報データが移動されているので、メモリカード１１０は「状態ＳＡ」となっている。

【０１４３】

一方、ステップＳ３０６′において、「複製リクエスト」が与えられていると判断された場合は、携帯電話機１００から携帯電話機１０２に対して複製受理が送信される（ステップＳ３７０）。携帯電話機１０２において、複製受理を受信すると（ステップＳ３７２）、処理が終了する（ステップＳ３７４）。

【０１４４】

このような構成とすることで、メモリカード自身が、セッションキーＫｓを送る側（携帯電話機１００）に、公開暗号化鍵ＫＰｍｅｄｉａ（１）およびＫＰｍｅｄｉａ（２）を送信した上で、移動動作を行なうこと、および複製動作を行なうことが可能となる。

【０１４５】

［実施の形態２］

実施の形態２のデータ配信システムにおいては、実施の形態１のデータ配信システムの構成と異なって、配信サーバ、携帯電話機およびメモリカードの各々が、独自のセッションキーを生成する構成となっていることを１つの特徴とする。すなわち、配信サーバまたは携帯電話機の発生するセッションキーをセッションキーＫｓとし、一方のメモリカード１２０の発生するセッションキーをセッションキーＫｓ１とし、メモリカード１２０と同様の構成を有する他方のメモリカード１２２の発生するセッションキーをセッションキーＫｓ２とする。

【０１４６】

すなわち、実施の形態２のデータ配信システムにおいては、システムを構成する機器の各々が、自身でセッションキーを生成し、データを受け取るとき、言い換えるとデータの送信先になっている場合には、相手方（送信元）に対して、まず、セッションキーを配送する。送信元は、この送信先から配送されたセッションキーでデータを暗号化し、この暗号化データを送信する。送信先では、自身で生成したセッションキーにより、受け取ったデータを復号化するという構成を１つの特徴とするものである。

【０１４７】

また、上記のような動作を実現するために、再生動作において、携帯電話機側がメモリカードの生成するセッションキーを受け取るための公開暗号化鍵をＫＰ

ｐとし、この公開暗号化鍵ＫＰｐで暗号化されたデータを復号化できる秘密復号鍵を鍵Ｋｐとする。

【０１４８】

図１１は、実施の形態２のメモリカード１２０に対応した配信サーバ１１の構成を示す概略ブロック図である。図３に示した配信サーバ１０の構成と異なる点は、データ処理部３１０における暗号化処理部３２２は、Ｋｓ発生部３１４からのセッションキーＫｓに基づいてではなく、携帯電話機に装着されたメモリカードからセッションキーＫｓ１、Ｋｓ２により暗号化されて送信され、復号処理部３１８により復号抽出されたセッションキー、たとえば、セッションキーＫｓ１に基づいて、暗号化処理部３２０の出力をさらに暗号化して、データバスＢＳ１を介して通信装置３５０に与える点である。

【０１４９】

配信サーバ１１のその他の点は、図３に示した実施の形態１の配信サーバ１０の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

【０１５０】

図１２は、実施の形態２における携帯電話機１０１の構成を説明するための概略ブロック図である。

【０１５１】

図４に示した携帯電話機１００の構成と異なる点は、まず、メモリカード１２０が装着されていること以外に、携帯電話機１０１は、公開暗号化鍵ＫＰｐを保持して、再生動作時に公開暗号化鍵ＫＰｐをデータバスＢＳ２に出力するＫＰｐ保持部１５２４を備える構成となっていることである。

【０１５２】

さらに、携帯電話機１０１は、秘密復号鍵Ｋｐを保持するＫｐ保持部１５２０と、このＫｐ保持部１５２０から与えられる秘密復号鍵Ｋｐに基づいて、データバスＢＳ２を介してメモリカード１２０から与えられる公開暗号化鍵ＫＰｐで暗号化されたセッションキーＫｓ１を復号し抽出する復号処理部１５２２とをさらに備える構成となっている。しかも、暗号化処理部１５０４は、この復号処理部

１５２２から与えられるセッションキーＫｓ１により、Ｋｓ発生部１５０２からの自身のセッションキーＫｓを暗号化してデータバスＢＳ２に出力する。

【０１５３】

携帯電話機１０１のその他の点は、図４に示した実施の形態１の携帯電話機１００の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

【０１５４】

図１３は、本発明の実施の形態２のメモリカード１２０の構成を説明するための概略ブロック図であり、実施の形態１の図５と対比される図である。

【０１５５】

メモリカード１２０の構成が、メモリカード１１０の構成と異なる点は、まず、メモリカード１２０は、このカード独自のセッションキーＫｓ１を発生するセッションキーＫｓ１発生部１４３２を備えることである。

【０１５６】

さらに、メモリカード１２０は、セッションキー発生回路１４３２で生成されたセッションキーＫｓ１を、暗号化してデータバスＢＳ３に与えるための暗号化処理部１４３０を備える。

【０１５７】

これに応じて、メモリカード１２０は、さらに、再生モードにおいて、形態電話機１０１の公開暗号化鍵ＫＰｐを受けて保持するＫＰｐ受理部１４０７と、移動モードにおいて、相手方（移動先）の公開暗号化鍵ＫＰｍｅｄｉａ（ｎ）を受けて保持するＫＰｍｅｄｉａ受理部１４０３と、このＫＰｍｅｄｉａ受理部１４０３の出力とＫＰｐ受理部１４０７の出力とを受けて、動作モードに応じていずれか一方を出力する切換えスイッチ１４３６を備える。切換えスイッチ１４３６は、接点ＰｉおよびＰｈとを有し、接点ＰｉはＫＰｐ受理部１４０７と、接点ＰｈはＫＰｍｅｄｉａ受理部１４０３とそれぞれ結合する。暗号化処理部１４３０は、切換えスイッチ１４３６から与えられる公開暗号化鍵ＫＰｍｅｄｉａ（ｎ）または公開暗号化鍵ＫＰｐのいずれかにより、Ｋｓ１発生部１４３２からのセッションキーＫｓ１を暗号化して、データバスＢＳ３に与える。

【０１５８】

すなわち、切換えスイッチ１４３６は、配信動作のとき、および移動動作において移動先となっているときは、未使用状態であり、再生動作の時は、接点Ｐｉの側に閉じており、移動動作において移動元となっているときは、接点Ｐｈの側に閉じている。

【０１５９】

メモリカード１２０は、さらに、接点Ｐｅ、ＰｆおよびＰｇを有し、復号処理部１４０４から与えられる音楽サーバからのセッションキーＫｓと、Ｋｓ１発生部１４３２の出力と、データバスＢＳ４から与えられる携帯電話機１０１からのセッションキーＫｓとを受けて、動作モードに応じていずれか１つを選択的に出力する切換えスイッチ１４３５を備える。接点Ｐｅには復号処理部１４０４からの出力が、接点ＰｆにはＫｓ１発生部１４３２の出力が、接点Ｐｇにはデータバスバス４がそれぞれ結合している。したがって、暗号化処理部１４０６と復号処理部１４１０は、この切換えスイッチ１４３５から与えられるキーに基づいて、それぞれ、暗号化処理および復号処理を行なう。

【０１６０】

すなわち、切換えスイッチ１４３５は、配信動作の場合に音楽サーバ３１からのセッションキーＫｓ１の抽出を行なうときは、接点Ｐｅの側に閉じており、配信動作の場合に音楽サーバ３１からの暗号化されたライセンスキーＫｃ、ライセンス情報データについてセッションキーＫｓ１による復号を行なうときは、接点Ｐｆの側に閉じている。切換えスイッチ１４３５は、再生動作において復号処理を行なうときは、接点Ｐｆの側に閉じており、再生動作において暗号化処理を行なうときは、接点Ｐｇの側に閉じている。切換えスイッチ１４３５は、移動動作において移動元となっている場合に復号処理を行なうときは、接点Ｐｆの側に閉じており、移動動作において移動元となっている場合に暗号化処理を行なうときは、接点Ｐｇの側に閉じている。切換えスイッチ１４３５は、移動動作において移動先となっている場合に移動元のセッションキーを受け取るときは、接点Ｐｅの側に閉じており、移動動作において移動先となっている場合にライセンスキーＫｃおよびライセンス情報データＬｉｃｅｎｓｅを受け取るときは、接点Ｐｆの

側に閉じている。

【０１６１】

メモリカード１２０は、さらに、接点Ｐａ、Ｐｂ、ＰｃおよびＰｄ　を有し、Ｋｓ１発生部１４３２から与えられる自身のセッションキーＫｓ１と、ＫＰｃａｒｄ保持部１４０５の出力と、データバスＢＳ５から与えられるライセンスキーＫｃと、暗号化処理部１４１４から与えられ、相手方の公開暗号化鍵ＫＰｃａｒｄ（ｎ）により暗号化されたライセンスキーＫｃおよびライセンス情報データＬｉｃｅｎｓｅを受けて、動作モードに応じていずれか１つを選択的に出力する切換えスイッチ１４０９を、切換えスイッチ１４０８の替わりに備える。

【０１６２】

接点ＰａにはＫｓ１発生部１４３２からの出力が、接点ＰｂにはＫＰｃａｒｄ（１）保持部１４０５の出力が、接点ＰｃにはデータバスＢＳ５が、接点Ｐｄには暗号化処理部１４１４の出力が、それぞれ結合している。したがって、暗号化処理部１４０６は、この切換えスイッチ１４０９から与えられるデータに対して、それぞれ、暗号化処理を行なう。

【０１６３】

すなわち、切換えスイッチ１４０９は、配信モードにおいて、配信先となっている場合に音楽サーバ３１に自身の公開暗号化鍵ＫＰｃａｒｄ（１）や自身のセッションキーＫｓ１を送信するときは、順次、接点Ｐｂの側および接点Ｐａの側に閉じる。切換えスイッチ１４０９は、再生モードのときは、接点Ｐｃの側に閉じており、移動モードにおいて移動元となっているときは、接点Ｐｄの側に閉じている。切換えスイッチ１４０９は、移動モードにおいて移動先となっている場合にも移動元に自身の公開暗号化鍵ＫＰｃａｒｄ（１）や自身のセッションキーＫｓ１を送信するときは、順次、接点Ｐｂの側および接点Ｐａの側に閉じる。

【０１６４】

図１４および図１５は、図１３で説明したメモリカード１２０を用いた配信モードを説明するための第１および第２のフローチャートである。

【０１６５】

図１４および図１５においても、ユーザ１が、メモリカード１２０を用いるこ

とで、音楽サーバ３１から音楽データの配信を受ける配信モードの動作を説明している。

【０１６６】

まず、ユーザ１の携帯電話機１０１から、ユーザによりタッチキー１１０８のキーボタンの操作等によって、配信リクエストがなされる（ステップＳ１００）。

【０１６７】

メモリカード１２０においては、この配信リクエストに応じて、ＫＰｍｅｄｉａ（１）保持部１４０１から、公開暗号化鍵ＫＰｍｅｄｉａ（１）を音楽サーバ３１に対して送信する（ステップＳ１０２）。さらに、メモリカード１２０においては、Ｋｓ１発生部１４３２によりセッションキーＫｓ１が生成される（ステップＳ１０９）。

【０１６８】

音楽サーバ３１では、メモリカード１２０から転送された配信リクエストならびに公開暗号化鍵ＫＰｍｅｄｉａ（１）を受信すると（ステップＳ１０４）、受信した公開暗号化鍵ＫＰｍｅｄｉａ（１）に基づいて、認証サーバ１２に対して照会を行ない、正規のメモリカードを用いたアクセスの場合は次の処理に移行し（ステップＳ１０６）、正規のメモリカードでない場合には、処理を終了する（ステップＳ１５４）。

【０１６９】

照会の結果、正規のメモリカードであることが確認されると、音楽サーバ３１では、セッションキー発生部３１４が、セッションキーＫｓを生成する。さらに、音楽サーバ３１内の暗号化処理部３１６が、受信した公開暗号化鍵ＫＰｍｅｄｉａ（１）により、このセッションキーＫｓを暗号化して暗号化セッションキー［Ｋｓ］Ｋｍｅｄｉａ（１）を生成する（ステップＳ１０８）。

【０１７０】

続いて、音楽サーバ３１は、暗号化セッションキー［Ｋｓ］Ｋｍｅｄｉａ（１）をデータバスＢＳ１に与える。通信装置３５０は、暗号化処理部３１６からの暗号化セッションキー［Ｋｓ］Ｋｍｅｄｉａ（１）を、通信網を通じて、携帯電

話機１０１のメモリカード１２０に対して送信する（ステップＳ１１０）。

【０１７１】

携帯電話機１０１が、暗号化セッションキー［Ｋｓ］Ｋｍｅｄｉａ（１）を受信すると（ステップＳ１１２）、メモリカード１２０においては、メモリインタフェース１２００を介して、データバスＢＳ３に与えられた受信データを、復号処理部１４０４が、秘密復号鍵Ｋｍｅｄｉａ（１）で復号処理することにより、セッションキーＫｓを復号し抽出する（ステップＳ１１４）。

【０１７２】

続いて、配信モードにおいては、切換えスイッチ１４０９は、接点ＰａまたはＰｂが順次閉じる状態が選択されるので、暗号化処理部１４０６は、接点Ｐａを介してセッションキー発生部１４３２から与えられるセッションキーＫｓ１と接点Ｐｂを介してＫＰｃａｒｄ（１）保持部１４０５から与えられる公開暗号化鍵ＫＰｃａｒｄ（１）（メモリカード１２０に対する公開暗号化鍵）とを、セッションキーＫｓにより暗号化し（ステップＳ１１６）、データ［ＫＰｃａｒｄ（１）、Ｋｓ１］Ｋｓを生成する（ステップＳ１１８）。

【０１７３】

携帯電話機１０１は、暗号化処理部１４０６により暗号化されたデータ［ＫＰｃａｒｄ（１）、Ｋｓ１］Ｋｓを音楽サーバ３１に対して送信する（ステップＳ１２０）。

【０１７４】

音楽サーバ３１では、通信装置３５０によりデータ［ＫＰｃａｒｄ（１）、Ｋｓ１］Ｋｓが受信され（ステップＳ１２２）、データバスＢＳ１に与えられたデータ［ＫＰｃａｒｄ（１）、Ｋｓ１］Ｋｓを復号処理部３１８が、セッションキーＫｓにより復号処理して、公開暗号化鍵ＫＰｃａｒｄ（１）およびセッションキーＫｓ１を復号抽出する（ステップＳ１２４）。

【０１７５】

続いて、配信制御部３１２は、配信情報データベース３０４等に保持されているデータを元に、ライセンスＩＤデータ等を含むライセンス情報データＬｉｃｅｎｓｅを生成する（ステップＳ１２６）。

【０１７６】

さらに、音楽サーバ３１は、暗号化コンテンツデータ［Ｄｃ］Ｋｃを配信情報データベース３０４より取得して、通信装置３５０を介して、メモリカード１２０に送信する（ステップＳ１２８）。

【０１７７】

携帯電話機１０１が暗号化コンテンツデータ［Ｄｃ］Ｋｃを受信すると（ステップＳ１３０）、メモリカード１２０においては、受信した暗号化コンテンツデータ［Ｄｃ］Ｋｃをそのままメモリ１４１２に格納する（ステップＳ１３２）。

【０１７８】

一方、音楽サーバ３１は、ライセンスキーＫｃを配信情報データベース３０４より取得し（ステップＳ１３４）、暗号化処理部３２０は、配信制御部３１２からのライセンスキーＫｃとライセンス情報データＬｉｃｅｎｓｅとを、復号処理部３１８より与えられた公開暗号化鍵ＫＰｃａｒｄ（１）により暗号化処理する（ステップＳ１３６）。

【０１７９】

暗号化処理部３２２は、暗号化処理部３２０により暗号化されたデータ［Ｋｃ、Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）を受取って、さらに、メモリカード１２０からのセッションキーＫｓ１により暗号化したデータをデータバスＢＳ１に与える。通信装置３５０は、暗号化処理部３２２により暗号化されたデータ［［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）］Ｋｓ１をメモリカード１２０に対して送信する。

【０１８０】

携帯電話機１０１がデータ［［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）］Ｋｓ１を受信すると（ステップＳ１４２）、メモリカード１２０においては、復号処理部１４１０が接点Ｐｆを介してＫｓ１発生部１４３２から与えられるセッションキーＫｓ１により復号処理を行ない、データ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）を抽出し、メモリ１４１２に格納する（ステップＳ１４６）。

【０１８１】

さらに、メモリカード１２０においては、コントローラ１４２０により制御さ

れて、復号処理部１４１６が、メモリ１４１２に格納されたデータ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）を復号し、復号されたライセンス情報データＬｉｃｅｎｓｅを、レジスタ１５００に格納する（ステップ１４８）。

【０１８２】

以上のような動作により、メモリカード１２０自身が、暗号化コンテンツデータを送る側（音楽サーバ３１）に、公開暗号化鍵ＫＰｍｅｄｉａ（１）およびセッションキーＫｓ１を送信した上で、配信を受けることができ、メモリカード１２０は、音楽情報を再生可能な状態となる。

【０１８３】

さらに、メモリカード１２０から音楽サーバ３１へは、配信受理が通知され、音楽サーバ３１で配信受理を受信すると（ステップＳ１５０）、課金データベース３０２にユーザ１の課金データが格納され（ステップＳ１５２）、処理が終了する（ステップＳ１５４）。

【０１８４】

図１６および図１７は、携帯電話機１０１内において、メモリカード１２０に保持された暗号化コンテンツデータから、音楽データであるコンテンツデータを復号化し、音楽として外部に出力するための再生モードを説明する第１および第２のフローチャートである。

【０１８５】

図１６および図１７を参照して、携帯電話機のタッチキー１１０８等からのユーザ１の指示により、再生リクエストがメモリカード１２０に対して出力される（ステップＳ２００）。

【０１８６】

メモリカード１２０においては、この再生リクエストに応じて、コントローラ１４２０は、レジスタ１５００に保持されるライセンス情報データＬｉｃｅｎｓｅに基づいて、復号可能なデータに対するリクエストであるかを判断し（ステップＳ２０２）、再生可能と判断した場合は、再生可能通知を携帯電話機１０１に対して送信する（ステップＳ２４０）。一方、再生不可能と判断した場合は、処理を終了する（ステップＳ２８０）。

【０１８７】

再生可能と判断され、メモリカード１２０から再生可能通知が送信された場合、携帯電話機１０１では、公開暗号化鍵ＫＰｐをメモリカード１２０に送信し（ステップＳ２４２）、Ｋｓ発生部１５０２においてセッションキーＫｓを生成する（ステップＳ２４４）。

【０１８８】

一方、メモリカード１２０も、セッションキーＫｓ１を生成する（ステップＳ２４０）。メモリカード１２０は、さらに、データバスＢＳ２を介して携帯電話機１０１から受けとった公開暗号化鍵ＫＰｐによりセッションキーＫｓ１を暗合化し（ステップＳ２４８）、生成された暗号化セッションキー［Ｋｓ１］Ｋｐを携帯電話機１０１に対して送信する（ステップＳ２５０）。

【０１８９】

携帯電話機１０１では、メモリカード１２０からの暗号化セッションキー［Ｋｓ１］Ｋｐを受信すると、復号処理部１５２２が、秘密復号鍵Ｋｐにより復号化してメモリカード１２０で生成したセッションキーＫｓ１を抽出する（ステップＳ２５２）。続いて、携帯電話機１０１の暗号化処理部１５０４は、携帯電話機１０１で生成したセッションキーＫｓをセッションキーＫｓ１により暗号化して、暗号化セッションキー［Ｋｓ］Ｋｓ１を生成し（ステップＳ２５４）、この暗号化セッションキー［Ｋｓ］Ｋｓ１をメモリカード１２０に対して送信する（ステップＳ２５６）。

【０１９０】

メモリカード１２０は、データバスＢＳ２を介して、携帯電話機１０１により生成された暗号化セッションキー［Ｋｓ］Ｋｓ１を受け取り、セッションキーＫｓ１により復号し、携帯電話機１０１で生成したセッションキーＫｓを抽出する（ステップＳ２５８）。

【０１９１】

続いて、メモリカード１２０は、メモリ１４１２から、暗号化されているデータ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）を読み出し、復号処理部１４１６が復号処理を行なう（ステップＳ２６０）。

【０１９２】

秘密復号鍵Ｋｃａｒｄ（１）により、メモリ１４１２から読み出されたデータを復号可能な場合（ステップＳ２６２）、ライセンスキーＫｃが抽出される（ステップＳ２６４）。一方、復号不可能の場合、処理は終了する（ステップＳ２８０）。

【０１９３】

メモリ１４１２から読み出されたデータを復号可能な場合は、さらに、レジスタ１５００内のライセンス情報データＬｉｃｅｎｓｅのうち、再生回数に関するデータが変更される（ステップＳ２６６）。

【０１９４】

続いて、メモリカード１２０においては、暗号化処理部１４０６が、抽出したセッションキーＫｓにより、ライセンスキーＫｃを暗号化し（ステップＳ２６８）、暗号化ライセンスキー［Ｋｃ］Ｋｓをデータバスｂｓ２に与える（ステップＳ２７０）。

【０１９５】

携帯電話機１０１の復号処理部１５０６は、セッションキーＫｓにより復号化処理を行なうことにより、ライセンスキーＫｃを取得する（ステップＳ２７２）。

【０１９６】

続いて、メモリカード１２０は、暗号化コンテンツデータ［Ｄｃ］Ｋｃをメモリ１４１２から読み出し、データバスｂｓ２に与える（ステップＳ２７４）。

【０１９７】

携帯電話機１０１の音楽再生部１５０８は、暗号化コンテンツデータ［Ｄｃ］Ｋｃを、抽出されたライセンスキーＫｃにより復号処理して平文のコンテンツデータを生成し（ステップＳ２７６）、音楽信号を再生して混合部１５１０に与える（ステップＳ２７６）。デジタルアナログ変換部１５１２は、混合部１５１０からの音楽信号を受け取って変換し、外部に再生された音楽を出力し、処理が終了する（ステップＳ２３２）。

【０１９８】

このような構成とすることで、メモリカード自身および携帯電話自身が、それぞれセッションキーＫｓ１またはＫｓを生成し、これにより暗号化されたデータの授受を行なった上で、再生動作を行なうことが可能となる。

【０１９９】

図１８および図１９は、２つのメモリカード間において、コンテンツデータおよびキーデータ等の移動モードまたは複製モードを行なう処理を説明するための第１および第２のフローチャートである。

【０２００】

まず、携帯電話機１０１と同様の構成を有する携帯電話機１０３が送信側であり、携帯電話機１０１が受信側であるものとする。また、携帯電話機１０３にも、メモリカード１２０と同様の構成を有するメモリカード１２２が装着されているものとする。

【０２０１】

携帯電話機１０３は、まず、自身の側のメモリカード１２２および携帯電話機１０１に対して、移動リクエストまたは複製リクエストを出力する（ステップＳ３００）。

【０２０２】

メモリカード１２２は、これに応じて、メモリ１４１２内の暗号化コンテンツデータ［Ｄｃ］Ｋｃを読み出して、メモリカード１２０に対して出力し（ステップＳ３０２）、一方、携帯電話機１０１は、携帯電話機１０３からのリクエストを受信し（ステップＳ３０１）、メモリカード１２０では、暗号化コンテンツデータ［Ｄｃ］Ｋｃをメモリ１４１２に格納する（ステップＳ３０４）。

【０２０３】

続いて、携帯電話機１０３および１０１においては、ステップＳ３００において与えられたリクエストが、「移動リクエスト」であるか「複製リクエスト」であるかが判断され（ステップＳ３０６、ステップＳ３０６′）、「移動リクエスト」である場合、メモリカード１２０は、公開暗号化鍵ＫＰｍｅｄｉａ（１）を携帯電話機１０１に出力し（ステップＳ３０８）、携帯電話機１０１は、公開暗号化鍵ＫＰｍｅｄｉａ（１）を携帯電話機１０３に対して送信する（ステップＳ

３１０）。

【０２０４】

携帯電話機１０３が、公開暗号化鍵ＫＰｍｅｄｉａ（１）を受信し（ステップＳ３１２）、メモリカード１２２に転送すると（ステップＳ３１３）、メモリカード１２２のＫｓ２発生回路１４３２は、セッションキーＫｓ２を生成し（ステップＳ３１４）、公開暗号化鍵ＫＰｍｅｄｉａ（１）を用いて、暗号化処理部１４３０がセッションキーＫｓ２を暗号化する（ステップＳ３１５）。

【０２０５】

携帯電話機１０３は、暗号化セッションキー［Ｋｓ２］ＫＰｍｅｄｉａ（１）を携帯電話機１０１に対して送信する（ステップＳ３１６）。携帯電話機１０１は、暗号化セッションキー［Ｋｓ２］ＫＰｍｅｄｉａ（１）を受信すると（ステップＳ３１８）、メモリカード１２０に伝達し、メモリカード１２０は、復号処理部１４０４が復号して、セッションキーＫｓ２を受理し、さらに、セッションキー生成部１４３２で、メモリカード１２０におけるセッションキーＫｓ１が生成される（ステップＳ３２０）。

【０２０６】

メモリカード１２０においては、セッションキーＫｓ２によりメモリカード１２０の公開暗号化鍵ＫＰｃａｒｄ（１）およびセッションキーＫｓ１を暗号化して（ステップＳ３２２）、携帯電話機１０１から携帯電話機１０３に対して暗号化されたデータ［ＫＰｃａｒｄ（１）、Ｋｓ１］Ｋｓ２を送信する（ステップＳ３２４）。携帯電話機１０３は、データ［ＫＰｃａｒｄ（１）、Ｋｓ１］Ｋｓ２を受信し（ステップＳ３２６）、メモリカード１２２に転送する。

【０２０７】

メモリカード１２２においては、復号処理部１４１０が、メモリカード１２０から送信された暗号化データ［ＫＰｃａｒｄ（１）、Ｋｓ１］Ｋｓ２をセッションキーＫｓ２により復号化して、メモリカード１２０の公開暗号化鍵ＫＰｃａｒｄ（１）、セッションキーＫｓ１を復号抽出する（ステップＳ３３０）。

【０２０８】

続いて、メモリカード１２２においては、メモリ１４１２からメモリカード１

２２の公開暗号化鍵ＫＰｃａｒｄ（２）により暗号化されているライセンスキーＫｃ、ライセンス情報データＬｉｃｅｎｓｅに対応する［Ｋｃ、Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（２）が読み出される（ステップＳ３３２）。

【０２０９】

続いて、メモリカード１２２の復号処理部１４１６が、秘密復号鍵Ｋｃａｒｄ（２）により、［Ｋｃ、Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（２）を復号処理する（ステップＳ３３４）。

【０２１０】

メモリカード１２２のコントローラ１４２０は、このようにして復号されたライセンス情報データＬｉｃｅｎｓｅの値を、レジスタ１５００内のデータ値と置換する（ステップＳ３３６）。

【０２１１】

さらに、メモリカード１２２の暗号化処理部１４１４は、復号処理部1,4１０において抽出されたメモリカード１２０における公開暗号化鍵ＫＰｃａｒｄ（１）により、ライセンスキーＫｃ、ライセンス情報データＬｉｃｅｎｓｅとを暗号化する（ステップＳ３３８）。

【０２１２】

メモリカード１２２の暗号化処理部１４１４により暗号化されたデータは、切換えスイッチ１４０９（接点Ｐｄが閉じている）を介して、さらに、暗号化処理部１４０６に与えられ、メモリカード１２２の暗号化処理部１４０６は、データ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）をセッションキーＫｓ１により暗号化してデータ［［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）］Ｋｓ１を生成する（ステップＳ３４０）。

【０２１３】

続いて、メモリカード１２２は、携帯電話機１０３に対してデータ［［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）］Ｋｓ１を出力し（ステップＳ３４２）、携帯電話機１０３はデータ［［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）］Ｋｓ１を携帯電話機１０１に対して送信する（ステップＳ３４４）。

【０２１４】

携帯電話機１０１が受信したデータ［［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）］Ｋｓ１は（ステップＳ３４６）、メモリカード１２０に対して伝達され、メモリカード１２０の復号処理部１４１０は、暗号化されたデータ［［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）］Ｋｓ１を復号して、データ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）を受理する（ステップＳ３４８）。

【０２１５】

メモリカード１２０においては、復号処理部１４１０により、セッションキーＫｓ１に基づいて復号化処理されたデータ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）をメモリ１４１２に格納する（ステップＳ３５０）。さらに、メモリカード１２０においては、復号処理部１４１６が、秘密復号鍵Ｋｃａｒｄ（１）に基づいて、データ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）を復号し、復号されたライセンス情報データＬｉｃｅｎｓｅをレジスタ１５００に格納する（ステップＳ３５２）。

【０２１６】

以後の移動モードにおける処理ならびに複製モードにおけるメモリカード１２０および１２２の処理は、図９および図１０で説明した実施の形態１のメモリカード１１０、１１２等の処理と同様であるので、その説明は繰り返さない。

【０２１７】

このような構成とすることで、移動元および移動先のメモリカード自身が、セッションキーをそれぞれ生成した上で、移動モードを行なうが可能となる。

【０２１８】

したがって、データバス上等で伝達されるデータのライセンスキーＫｃおよびライセンス情報データＬｉｃｅｎｓｅを暗号化する鍵が、セッションごとに、かつ、機器ごとに変更されるので、ライセンスキーＫｃおよびライセンス情報データＬｉｃｅｎｓｅの授受のセキュリティが一層向上するという効果がある。

【０２１９】

しかも、以上のような構成を用いることで、たとえば、メモリカード１２２からメモリカード１２０へのデータの移動を、上述したようなセッションキー発生回路１５０２を有する携帯電話端末を介さずに、メモリカードとメモリカードと

を接続可能なインターフェース機器により行なうことも可能となり、ユーザの利便性が一層向上するという効果がある。

【０２２０】

ここで、移動時には、再生回数を制限するライセンス情報データ内の設定については、メモリ１４１２に記録されたライセンス情報データを、レジスタ１５００にて再生の都度修正された再生回数を記録したライセンス情報データに変更することで、ライセンス情報データを更新する。このようにして、メモリカード間をコンテンツデータが移動しても、再生回数に制限があるコンテンツデータの再生回数は、配信時に決められた再生回数の制限を越えることがないようにすることが可能である。

【０２２１】

［実施の形態３］

実施の形態３のデータ配信システムにおいては、ユーザは、配信キャリアである携帯電話会社から暗号化コンテンツデータの配信を受けるのではなく、たとえば、街頭などに設置されているコンテンツデータ販売機から暗号化コンテンツデータの供給を受ける構成となっていることを１つの特徴とする。

【０２２２】

図２０は、このような実施の形態３のデータ配信システムの構成を説明するための概念図である。なお、携帯電話機１００およびメモリカード１１０の構成は実施の形態１で説明したものと同様であるので、その説明は繰り返さない。

【０２２３】

図２０を参照して、コンテンツデータ販売機２０００は、ユーザに対して配信作業における案内等を出力するためのディスプレイ２００２と、ユーザから指示を入力するためのキーボード２００４と、料金投入口２００６と、携帯電話機１００とコネクタ１１２０を介してデータの授受を行なうための外部コネクタ２０１０とを備える。さらに、コンテンツデータ販売機２０００は、携帯電話網等の通信路を介して、販売記録等を管理するための管理サーバ２２００と接続している。

【０２２４】

図２１は、実施の形態３のコンテンツデータ販売機２０００の構成を示す概略ブロック図である。コンテンツデータ販売機２０００は、上述したように、ディスプレイ２００２と、キーボード２００４と、料金投入口２００６からの投入金を受ける料金受理部２０２０と、外部コネクタ２０１０と、コネクタ２０１０とデータバスとの間に設けられるインターフェース部２０１２と、コンテンツデータ（音楽データ）を所定の方式に従って暗号化したデータや、ライセンス情報データ等の配信情報を保持するための配信情報データベース３０４と、管理サーバ２２００との間で情報の授受をするための通信装置３６０と、配信情報データベース３０４および管理サーバ２２００からのデータをデータバスＢＳ１を介して受取り、所定の暗号化処理を行なうためのデータ処理部２１００とを備える。

【０２２５】

データ処理部２１００中は、実施の形態１と同様に、データバスＢＳ１上のデータに応じて、データ処理部２１００の動作を制御するための配信制御部３１２と、配信制御部３１２に制御されて、セッションキーＫｓを発生するためのセッションキー発生部３１４と、セッションキー発生部３１４より生成されたセッションキーＫｓを、カード媒体に固有な公開暗号化鍵ＫＰｍｅｄｉａ（ｎ）により暗号化して、データバスＢＳ１に与えるための暗号化処理部３１６と、各ユーザの携帯電話機においてセッションキーＫｓにより暗号化されたうえでコネクタ２０１０から与えられたデータをデータバスＢＳ１を介して受けて、復号処理を行なう復号処理部３１８と、復号処理部３１８により抽出された公開暗号化鍵ＫＰｃａｒｄ（ｎ）を用いて、ライセンス情報データを配信制御部３１２に制御されて暗号化するための暗号化処理部３２０と、暗号化処理部３２０の出力を、さらにセッションキーＫｓにより暗号化して、データバスＢＳ１を介してコネクタ２０１０に与える暗号化処理部３２２とを含む。

【０２２６】

図２２および図２３は、図２０および図２１で説明したデータ配信システムにおける配信モードを説明するための第１および第２のフローチャートである。

【０２２７】

図２２および図２３においては、ユーザ１が、メモリカード１１０を用いるこ

とで、コンテンツデータ販売機２０００から音楽データの配信を受ける場合の動作を説明している。

【０２２８】

まず、ユーザが、コンテンツデータ販売機２０００のキーボード２００４のキーボタンの操作等によって、配信リクエストを指示する（ステップＳ４００）。コンテンツデータ販売機２０００は、メモリカード１１０に対して公開暗号化鍵ＫＰｍｅｄｉａ（１）の送信依頼を出力する（ステップＳ４０２）。

【０２２９】

メモリカード１１０においては、この公開暗号化鍵ＫＰｍｅｄｉａ（１）の送信依頼に応じて、ＫＰｍｅｄｉａ（１）保持部１４０１から、公開暗号化鍵ＫＰｍｅｄｉａ（１）を携帯電話機１００に対して出力する（ステップＳ４０６）。

【０２３０】

携帯電話機１００がコンテンツデータ販売機２０００に公開暗号化鍵ＫＰｍｅｄｉａ（１）を送信し（ステップＳ４０８）、コンテンツデータ販売機２０００が、メモリカード１１０から転送された公開暗号化鍵ＫＰｍｅｄｉａ（１）を受信すると（ステップＳ４１０）、ディスプレイ２００２を介してユーザに料金投入を案内し、料金徴収を行なう（ステップＳ４１２）。続いて、コンテンツデータ販売機２０００は、セッションキー発生部３１４が、セッションキーＫｓを生成する。さらに、コンテンツデータ販売機２０００内の暗号化処理部３１６が、受信した公開暗号化鍵ＫＰｍｅｄｉａ（１）により、このセッションキーＫｓを暗号化して暗号化セッションキー［Ｋｓ］Ｋｍｅｄｉａ（１）を生成する（ステップＳ４１４）。

【０２３１】

続いて、コンテンツデータ販売機２０００は、暗号化セッションキー［Ｋｓ］Ｋｍｅｄｉａ（１）をデータバスＢＳ１に与え、コネクタ２０１０から出力する（ステップＳ４１６）。携帯電話機１００は、この暗号化セッションキー［Ｋｓ］Ｋｍｅｄｉａ（１）を受信すると、メモリカード１１０に転送する（ステップＳ４１８）。

【０２３２】

メモリカード１１０においては、メモリインタフェース１２００を介して、データバスＢＳ３に与えられた暗号化セッションキー［Ｋｓ］Ｋｍｅｄｉａ（１）を、復号処理部１４０４が、秘密復号鍵Ｋｍｅｄｉａ（１）により復号処理することにより、セッションキーＫｓを復号し抽出する（ステップＳ４２０）。

【０２３３】

続いて、配信モードにおいては、切換えスイッチ１４０８は、接点Ｐａが閉じる状態が選択されているので、暗号化処理部１４０６は、接点Ｐａを介してＫＰｃａｒｄ（１）保持部１４０５から与えられる公開暗号化鍵ＫＰｃａｒｄ（１）を、セッションキーＫｓにより暗号化し（ステップＳ４２２）、データ［ＫＰｃａｒｄ（１）］Ｋｓを生成する（ステップＳ４２４）。

【０２３４】

携帯電話機１００は、暗号化処理部１４０６により暗号化されたデータ［ＫＰｃａｒｄ（１）］Ｋｓをコンテンツデータ販売機２０００に対して送信する（ステップＳ４２６）。

【０２３５】

コンテンツデータ販売機２０００では、コネクタ２０１０を介してデータ［ＫＰｃａｒｄ（１）］Ｋｓが受信され（ステップＳ４２８）、データバスＢＳ１に与えられたデータ［ＫＰｃａｒｄ（１）］Ｋｓを復号処理部３１８が、セッションキーＫｓにより復号処理して、公開暗号鍵ＫＰｃａｒｄ（１）を復号抽出する（ステップＳ４３０）。

【０２３６】

続いて、配信制御部３１２は、配信情報データベース３０４等に保持されているデータを元に、ライセンスＩＤデータ等を含むライセンス情報データＬｉｃｅｎｓｅを生成する（ステップＳ４３２）。

【０２３７】

さらに、コンテンツデータ販売機２０００は、暗号化コンテンツデータ［Ｄｃ］Ｋｃを配信情報データベース３０４より取得して、コネクタ２０１０を介して、携帯電話機１００に送信する（ステップＳ４３４）。

【０２３８】

携帯電話機１００が暗号化コンテンツデータ［Ｄｃ］Ｋｃを受信すると（ステップＳ４３６）、メモリカード１１０においては、受信した暗号コンテンツデータ［Ｄｃ］Ｋｃをそのままメモリ１４１２に格納する（ステップＳ４３８）。

【０２３９】

一方、コンテンツデータ販売機２０００は、ライセンスキーＫｃを配信情報データベース３０４より取得し（ステップＳ４４０）、暗号化処理部３２０は、配信制御部３１２からのライセンスキーＫｃとライセンス情報データＬｉｃｅｎｓｅとを、復号処理部３１８より与えられた公開暗号化鍵ＫＰｃａｒｄ（１）により暗号化処理する（ステップＳ４４２）。

【０２４０】

暗号化処理部３２２は、暗号化処理部３２０により暗号化されたデータ［Ｋｃ、Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）を受取って、さらにセッションキーＫｓにより暗号化したデータをデータバスＢＳ１に与え、暗号化処理部３２２により暗号化されたデータ［［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）］Ｋｓがメモリカード１１０に対して送信される（ステップＳ４４６）。

【０２４１】

携帯電話機１００がデータ［［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）］Ｋｓを受信すると（ステップＳ４４８）、メモリカード１１０においては、復号処理部１４１０がセッションキーＫｓにより復号処理を行ない、データ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）を抽出し、メモリ１４１２に格納する（ステップＳ４５２）。

【０２４２】

さらに、メモリカード１１０においては、コントローラ１４２０により制御されて、復号処理部１４１６が、メモリ１４１２に格納されたデータ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）を復号し、復号されたライセンス情報データＬｉｃｅｎｓｅを、レジスタ１５００に格納する（ステップＳ４５８）。

【０２４３】

以上のような動作により、メモリカード自身が、セッションキーＫｓを送る側（コンテンツデータ販売機２０００）に、公開暗号化鍵ＫＰｍｅｄｉａ（１）を

送信した上で、配信を受けることができ、メモリカード１１０に格納された暗号化コンテンツデータを用いて音楽を再生可能な状態となる。

【０２４４】

さらに、メモリカード１１０からコンテンツデータ販売機２０００へは、携帯電話機１００を介して配信受理が通知され（ステップＳ４６０）、コンテンツデータ販売機２０００で配信受理を受信すると（ステップＳ４６２）、管理サーバに販売記録が送信され（ステップＳ４６４）、処理が終了する（ステップＳ４６６）。

【０２４５】

以上のような構成により、ユーザは、より簡易に暗号化された音楽データ等の配信を受けることができる。

【０２４６】

［実施の形態３の変形例］

実施の形態３のデータ配信システムにおいては、メモリカード１１０は、携帯電話機１００を介して、コンテンツデータ販売機２０００から暗号化コンテンツデータの配信を受ける構成であった。

【０２４７】

しかしながら、図２１に示したコンテンツデータ販売機２０００の構成において、コネクタ２０１０の代わりに、メモリカード１１０との間のインターフェースのためのメモリスロットを設ける構成とすれば、携帯電話機１００を介することなく、メモリカード１１０とコンテンツデータ販売機２０００とが直接データの授受を行なうことが可能である。

【０２４８】

図２４は、このような実施の形態３の変形例のコンテンツデータ販売機２００１の構成を示す概念図である。図２０に示した実施の形態３のコンテンツデータ販売機２０００の構成と異なる点は、外部コネクタ２０１０の代わりに、メモリカードを挿入できるカードスロット２０３０が設けられ、このカードスロット２０３０がインターフェース部２０１２を介して、データバスＢＳ１とデータの授受をする構成となっている点である。

【０２４９】

図２５および図２６は、実施の形態３の変形例のデータ配信システムにおける配信モードを説明するための第１および第２のフローチャートである。

【０２５０】

図２２および図２３に示した実施の形態３の配信モードとは、携帯電話機１００を介さずに、メモリカード１１０とコンテンツデータ販売機２００１がデータの授受をする点を除いては、同様の処理であるので、同一処理には同一符号を付して、その説明は繰り返さない。

【０２５１】

以上のような構成および動作により、一層簡易に、ユーザは暗号化された音楽データ等の配信を受けることができる。

【０２５２】

しかも、メモリカードが独立して、暗号化コンテンツデータの配信を受け、格納できるので、コンテンツデータの再生を行なう手段の選択の幅が広がり、よりユーザの利便性が向上するという利点もある。

【０２５３】

［実施の形態４］

図２７は、実施の形態４のコンテンツデータ販売機３０００の構成を説明するための概略ブロック図である。図２１に示したコンテンツデータ販売機２０００の構成と異なる点は、対象となるメモリカードが実施の形態２のメモリカード１２０であり、かつ使用される端末が携帯電話機１０１である点、およびこれに対応して、データ処理部２１００における暗号化処理部３２２は、Ｋｓ発生部３１４からのセッションキーＫｓに基づいてではなく、携帯電話機に装着されたメモリカードからセッションキーＫｓにより暗号化されて送信され、復号処理部３１８により復号抽出されたセッションキー、たとえば、セッションキーＫｓ１に基づいて、暗号化処理部３２０の出力をさらに暗号化して、データバスＢＳ１を介してインターフェース部２０１２およびコネクタ２０１０に与える点である。

【０２５４】

コンテンツデータ販売機３０００のその他の点は、図２１に示した実施の形態

３のコンテンツデータ販売機２０００の構成の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

【０２５５】

また、携帯電話機１０１およびメモリカード１１０の構成も実施の形態２で説明したものと同様であるので、その説明も繰り返さない。

【０２５６】

図２８および図２９は、図２７で説明したデータ配信システムにおける配信モードを説明するための第１および第２のフローチャートである。

【０２５７】

図２８および図２９においては、ユーザ１が、メモリカード１２０を用いることで、コンテンツデータ販売機３０００から音楽データの配信を受ける場合の動作を説明している。

【０２５８】

まず、ユーザが、コンテンツデータ販売機３０００のキーボード２００４のキーボタンの操作等によって、配信リクエストを指示する（ステップＳ５００）。コンテンツデータ販売機３０００は、メモリカード１１０に対して公開暗号化鍵ＫＰｍｅｄｉａ（１）の送信依頼を出力する（ステップＳ５０２）。

【０２５９】

メモリカード１２０においては、この公開暗号化鍵ＫＰｍｅｄｉａ（１）の送信依頼に応じて、ＫＰｍｅｄｉａ（１）保持部１４０１から、公開暗号化鍵ＫＰｍｅｄｉａ（１）をコンテンツデータ販売機３０００に対して送信する（ステップＳ５０６）。さらに、メモリカード１２０においては、Ｋｓ１発生部１４３２によりセッションキーＫｓ１が生成される（ステップＳ５１５）。

【０２６０】

携帯電話機１０１がコンテンツデータ販売機３０００に公開暗号化鍵ＫＰｍｅｄｉａ（１）を送信し（ステップＳ５０８）、コンテンツデータ販売機３０００が、メモリカード１２０から転送された公開暗号化鍵ＫＰｍｅｄｉａ（１）を受信すると（ステップＳ５１０）、ディスプレイ２００２を介してユーザに料金投入を案内し、料金徴収を行なう（ステップＳ５１２）。続いて、コンテンツデー

タ販売機３０００は、セッションキー発生部３１４が、セッションキーＫｓを生成する。さらに、コンテンツデータ販売機３０００内の暗号化処理部３１６が、受信した公開暗号化鍵ＫＰｍｅｄｉａ（１）により、このセッションキーＫｓを暗号化して暗号化セッションキー［Ｋｓ］Ｋｍｅｄｉａ（１）を生成する（ステップＳ５１４）。

【０２６１】

続いて、コンテンツデータ販売機３０００は、暗号化セッションキー［Ｋｓ］Ｋｍｅｄｉａ（１）をデータバスＢＳ１に与え、コネクタ２０１０から出力する（ステップＳ４１６）。携帯電話機１０１は、この暗号化セッションキー［Ｋｓ］Ｋｍｅｄｉａ（１）を受信すると、メモリカード１２０に転送する（ステップＳ５１８）。

【０２６２】

メモリカード１２０においては、メモリインタフェース１２００を介して、データバスＢＳ３に与えられた暗号化セッションキー［Ｋｓ］Ｋｍｅｄｉａ（１）を、復号処理部１４０４が、秘密復号鍵Ｋｍｅｄｉａ（１）により復号処理することにより、セッションキーＫｓを復号し抽出する（ステップＳ５２０）。

【０２６３】

続いて、暗号化処理部１４０６は、ＫＰｃａｒｄ（１）保持部１４０５から与えられる公開暗号化鍵ＫＰｃａｒｄ（１）およびＫｓ１発生部１４３２からのセッションキーＫｓ１を、セッションキーＫｓにより暗号化し（ステップＳ５２２）、データ［ＫＰｃａｒｄ（１）、Ｋｓ１］Ｋｓを生成する（ステップＳ５２４）。

【０２６４】

携帯電話機１０１は、暗号化処理部１４０６により暗号化されたデータ［ＫＰｃａｒｄ（１）、Ｋｓ１］Ｋｓをコンテンツデータ販売機３０００に対して送信する（ステップＳ５２６）。

【０２６５】

コンテンツデータ販売機３０００では、コネクタ２０１０を介してデータ［ＫＰｃａｒｄ（１）、Ｋｓ１］Ｋｓが受信され（ステップＳ５２８）、データバス

ＢＳ１に与えられたデータ［ＫＰｃａｒｄ（１）、Ｋｓ１］Ｋｓを復号処理部３１８が、セッションキーＫｓにより復号処理して、公開暗号化鍵ＫＰｃａｒｄ（１）およびセッションキーＫｓ１を復号抽出する（ステップＳ５３０）。

【０２６６】

続いて、配信制御部３１２は、配信情報データベース３０４等に保持されているデータを元に、ライセンスＩＤデータ等を含むライセンス情報データＬｉｃｅｎｓｅを生成する（ステップＳ５３２）。

【０２６７】

さらに、コンテンツデータ販売機３０００は、暗号化コンテンツデータ［Ｄｃ］Ｋｃを配信情報データベース３０４より取得して、コネクタ２０１０を介して、携帯電話機１０１に送信する（ステップＳ５３４）。

【０２６８】

携帯電話機１０１が暗号化コンテンツデータ［Ｄｃ］Ｋｃを受信すると（ステップＳ５３６）、メモリカード１２０においては、受信した暗号化コンテンツデータ［Ｄｃ］Ｋｃをそのままメモリ１４１２に格納する（ステップＳ５３８）。

【０２６９】

一方、コンテンツデータ販売機３０００は、ライセンスキーＫｃを配信情報データベース３０４より取得し（ステップＳ５４０）、暗号化処理部３２０は、配信制御部３１２からのライセンスキーＫｃとライセンス情報データＬｉｃｅｎｓｅとを、復号処理部３１８より与えられた公開暗号化鍵ＫＰｃａｒｄ（１）により暗号化処理する（ステップＳ５４２）。

【０２７０】

暗号化処理部３２２は、暗号化処理部３２０により暗号化されたデータ［Ｋｃ、Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）を受取って、さらにセッションキーＫｓ１により暗号化したデータをデータバスＢＳ１に与え、暗号化処理部３２２により暗号化されたデータ［［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）］Ｋｓ１が携帯電話機１０１に対して出力される（ステップＳ５４６）。

【０２７１】

携帯電話機１０１がデータ［［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）］Ｋ

ｓ１を受信すると（ステップＳ５４８）、メモリカード１２０においては、復号処理部１４１０がセッションキーＫｓ１により復号処理を行ない、データ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）を抽出し、メモリ１４１２に格納する（ステップＳ５５２）。

【０２７２】

以下の処理は、図２２および図２３に示した実施の形態３の処理と同様であるので、その説明は繰り返さない。

【０２７３】

以上のような構成により、ユーザは、より簡易に暗号化された音楽データ等のコンテンツデータ配信を受けることができる。

【０２７４】

しかも、データバス上等で伝達されるデータの暗号化キーが、セッションごとに、かつ、機器ごとに変更されるので、データ授受のセキュリティが一層向上するという効果がある。

【０２７５】

［実施の形態４の変形例］

実施の形態４のデータ配信システムにおいては、メモリカード１２０は、携帯電話機１０１を介して、コンテンツデータ販売機３０００から暗号化コンテンツデータの配信を受ける構成であった。

【０２７６】

しかしながら、図２７に示したコンテンツデータ販売機３０００の構成において、実施の形態３の変形例と同様に、コネクタ２０１０の代わりに、メモリカード１２０との間のインターフェースのためにメモリスロットを設ける構成とすれば、携帯電話機１０１を介することなく、メモリカード１２０とコンテンツデータ販売機３０００とが直接データの授受を行なうことが可能である。

【０２７７】

このような実施の形態４の変形例のコンテンツデータ販売機３００１の構成は、データ処理部２１００の構成を除いて、図２４に示した実施の形態３の変形例の構成と同様である。

【０２７８】

すなわち、実施の形態４の変形例のコンテンツデータ販売機３００１の構成は、図２７に示した実施の形態４のコンテンツデータ販売機３０００の構成と異なり、外部コネクタ２０１０の代わりに、メモリカードを挿入できるカードスロット２０３０が設けられ、このカードスロット２０３０がインターフェース部２０１２を介して、データバスＢＳ１とデータの授受をする構成となっている。

【０２７９】

図３０および図３１は、実施の形態４の変形例のデータ配信システムにおける配信モードを説明するための第１および第２のフローチャートである。

【０２８０】

図２８および図２９に示した実施の形態３の配信モードとは、携帯電話機１０１を介さずに、メモリカード１２０とコンテンツデータ販売機３００１がデータの授受をする点を除いては、同様の処理であるので、同一処理には同一符号を付して、その説明は繰り返さない。

【０２８１】

以上のような構成および動作により、一層簡易に、ユーザは暗号化された音楽データ等の配信を受けることができる。

【０２８２】

しかも、メモリカードが独立して、暗号化コンテンツデータの配信を受け、格納できるので、音楽の再生を行なう手段の選択の幅が広がり、よりユーザの利便性が向上するという利点もある。

【０２８３】

［実施の形態５］

実施の形態５の配信サーバ１２、携帯電話機１０５およびメモリカード１４０は、以下に説明するように、実施の形態２の配信サーバ１１、携帯電話機１０１およびメモリカード１２０の構成とは、以下の点で異なることを特徴とする。

【０２８４】

すなわち、実施の形態５の携帯電話機１０５では、たとえば、あらかじめ配信システムにおける認証機構等の管理部門にこの携帯電話機１０５を登録する際に

、この携帯電話機１０５に割当てられた公開暗号鍵ＫＰｐおよび証明データＣｒｔｆとを公開復号鍵（公開認証鍵）ＫＰｍａｓｔｅｒにより暗号化された形で記録保持する手段を有している。

【０２８５】

同様に、実施の形態５のメモリカード１４０でも、たとえば、あらかじめ配信システムにおける認証機構等の管理部門にこのメモリカード１４０を登録する際に、このメモリカードに割当てられた公開暗号鍵ＫＰｍｅｄｉａおよび証明データＣｒｔｆとを公開復号鍵（公開認証鍵）ＫＰｍａｓｔｅｒにより暗号化された形で記録保持する手段を有している。

【０２８６】

ここで、メモリカード１４０および実施の形態５の配信サーバ１２には、この公開復号鍵（公開認証鍵）ＫＰｍａｓｔｅｒを記録保持する手段を有している。この公開復号鍵（公開認証鍵）ＫＰｍａｓｔｅｒは、システム中でデータ出力を行なう全ての機器がセッションキーのやりとりに対して、相互にデータの授受を行なえる機器であることの証明と、セッションキーを相手方に送付する際に用いる暗号化鍵の獲得に用いるシステム共通の復号鍵である。

【０２８７】

以下、さらに、実施の形態５の携帯電話機１０５、メモリカード１４０および配信サーバ１２の構成をより詳しく説明する。

【０２８８】

図３２は、実施の形態５における携帯電話機１０５の構成を説明するための概略ブロック図である。

【０２８９】

図１２に示した実施の形態２の携帯電話機１０１の構成と異なる点は、ＫＰｐ保持部１５２４の替わりに、公開復号鍵（公開認証鍵）ＫＰｍａｓｔｅｒにより暗号化された、公開暗号鍵ＫＰｐおよび証明データＣｒｔｆを保持するための[ＫＰｐ，Ｃｒｔｆ] ＫＰｍａｓｔｅｒ保持部１５２５を備える構成となっていることである。

【０２９０】

携帯電話機１０５のその他の点は、図１２に示した実施の形態２の携帯電話機１０１の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

【０２９１】

図３３は、実施の形態５のメモリカード１４０に対応した配信サーバ１２の構成を示す概略ブロック図である。図１１に示した実施の形態２の配信サーバ１１の構成と異なる点は、データ処理部３１０は、公開復号鍵ＫＰｍａｓｔｅｒを保持するＫＰｍａｓｔｅｒ保持部３２４と、ＫＰｍａｓｔｅｒ保持部３２４から出力される公開復号鍵ＫＰｍａｓｔｅｒに基づいて、通信網から通信装置３５０を介してデータバスＢＳ１に与えられるデータを復号するための復号処理部３２６とをさらに備える構成となっている点である。暗号化処理部３１６は、復号処理部３２６での復号処理により抽出された公開暗号化鍵ＫＰｍｅｄｉａにより、Ｋｓ発生部３１４で発生されたセッションキーＫｓを暗号化し、また、配信制御部３１２は、復号処理部３２６での復号処理により抽出された証明データＣｒｔｆにより、配信を求めてきたメモリカードおよび携帯電話機が正規であるかの認証を行なう。

【０２９２】

配信サーバ１２のその他の点は、図１２に示した実施の形態２の配信サーバ１１の構成の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

【０２９３】

図３４は、本発明の実施の形態５のメモリカード１４０の構成を説明するための概略ブロック図であり、実施の形態２の図１３と対比される図である。

【０２９４】

実施の形態５のメモリカード１４０の構成が、実施の形態２のメモリカード１２０の構成と異なる点は、まず、メモリカード１４０は、公開暗号鍵ＫＰｍｅｄｉａおよび証明データＣｒｔｆとを公開復号鍵（公開認証鍵）ＫＰｍａｓｔｅｒにより暗号化された形で記録保持する[ＫＰｍｅｄｉａ，Ｃｒｔｆ] ＫＰｍａｓｔｅｒ保持部１４４２を備える構成となっていることである。一方で、切換えス

イッチ１４３６は省略され、[ＫＰｍｅｄｉａ，Ｃｒｔｆ] ＫＰｍａｓｔｅｒ保持部１４４２の出力は直接データバスＢＳ３に与えられる。

【０２９５】

さらに、メモリカード１４０は、公開復号鍵ＫＰｍａｓｔｅｒを記録保持するためのＫＰｍａｓｔｅｒ保持部１４５０と、ＫＰｍａｓｔｅｒ保持部１４５０から出力される公開復号鍵ＫＰｍａｓｔｅｒに基づいて、データバスＢＳ３上のデータを復号するための復号処理部１４５２とを備える。

【０２９６】

復号処理部１４５２での復号処理により抽出される公開暗号化鍵ＫＰｍｅｄｉａおよび証明データＣｒｔｆのうち、公開暗号化鍵ＫＰｍｅｄｉａは、暗号化処理部１４３０に与えられ、証明データＣｒｔｆは、データバスＢＳ５を介して、コントローラ１４２０に与えられる。

【０２９７】

メモリカード１４０のその他の構成は、図１３に示したメモリカード１２０の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

【０２９８】

［配信モード］

図３５および図３６は、図３４で説明したメモリカード１４０を用いた配信モードを説明するための第１および第２のフローチャートである。

【０２９９】

図３５および図３６においても、ユーザ１が、メモリカード１４０を装着した携帯電話機１０５にて配信サーバ１２からコンテンツデータの配信を受ける場合の動作を説明している。

【０３００】

まず、ユーザ１の携帯電話機１０５から、ユーザによりタッチキー１１０８のキーボタンの操作等によって、配信リクエストがなされる（ステップＳ１００）。

【０３０１】

また、メモリカード１４０において保持される公開暗号化鍵ＫＰｍｅｄｉａは、他のメモリカードにおける公開暗号化鍵ＫＰｍｅｄｉａと区別するために公開暗号化鍵ＫＰｍｅｄｉａ（１）としている。さらに、メモリカード１４０、携帯電話機１０５における証明データをそれぞれＣｒｔｆ（１）、Ｃｒｔｆ（ｐ）とする。

【０３０２】

メモリカード１４０においては、この配信リクエストに応じて、［ＫＰｍｅｄｉａ，Ｃｒｔｆ］ＫＰｍａｓｔｅｒ保持部１４４２から、公開暗号化鍵ＫＰｍｅｄｉａ（１）および証明データＣｒｔｆ（１）を暗号化したデータ［ＫＰｍｅｄｉａ（１），Ｃｒｔｆ（１）］ＫＰｍａｓｔｅｒを携帯電話機１０５に対して出力する（ステップＳ１０２′）。

【０３０３】

携帯電話機１０５では、メモリカード１４０からのデータ［ＫＰｍｅｄｉａ（１），Ｃｒｔｆ（１）］ＫＰｍａｓｔｅｒとともに、［ＫＰｐ，Ｃｒｔｆ］ＫＰｍａｓｔｅｒ保持部１５２５からのデータ［ＫＰｐ，Ｃｒｔｆ（ｐ）］ＫＰｍａｓｔｅｒ、配信リクエストを配信サーバ１２に対して送信する（ステップＳ１０３）。

【０３０４】

配信サーバ１２では、メモリカード１４０から転送された配信リクエストならびにデータ［ＫＰｐ，Ｃｒｔｆ（ｐ）］ＫＰｍａｓｔｅｒ、［ＫＰｍｅｄｉａ（１），Ｃｒｔｆ（１）］ＫＰｍａｓｔｅｒを受信すると（ステップＳ１０４′）、公開復号鍵ＫＰｍａｓｔｅｒにより復号処理部３２６が復号処理を行い、証明データＣｒｔｆ（１）、Ｃｒｔｆ（ｐ）、公開暗号化鍵ＫＰｐ、公開暗号化鍵ＫＰｍｅｄｉａ（１）の抽出を行なう（ステップＳ１０５）。

【０３０５】

復号された証明データＣｒｔｆ（１）およびＣｒｔｆ（ｐ）に基づいて、配信制御部３１２は、配信サーバ１２に対して照会を行ない、メモリカードと携帯電話機の証明データＣｒｔｆ（１）およびＣｒｔｆ（ｐ）がともに正規の証明データの場合は次の処理に移行し（ステップＳ１０６′）、いずれかが正規の証明デ

ータでない場合には、処理を終了する（ステップＳ１５４）。

【０３０６】

照会の結果、正規の証明データであることが確認されると、配信サーバ１２では、セッションキー発生部３１４が、セッションキーＫｓを生成する。さらに、配信サーバ１２内の暗号化処理部３１６が、受信した公開暗号化鍵ＫＰｍｅｄｉａ（１）により、このセッションキーＫｓを暗号化して暗号化セッションキー［Ｋｓ］Ｋｍｅｄｉａ（１）を生成する（ステップＳ１０８）。

【０３０７】

続いて、配信サーバ１２は、暗号化セッションキー［Ｋｓ］Ｋｍｅｄｉａ（１）をデータバスＢＳ１に与える。通信装置３５０は、暗号化処理部３１６からの暗号化セッションキー［Ｋｓ］Ｋｍｅｄｉａ（１）を、通信網を通じて、携帯電話機１０５のメモリカード１４０に対して送信する（ステップＳ１１０）。

【０３０８】

携帯電話機１０５が、暗号化セッションキー［Ｋｓ］Ｋｍｅｄｉａ（１）を受信すると（ステップＳ１１２）、メモリカード１４０においては、メモリインタフェース１２００を介して、データバスＢＳ３に与えられた受信データを、復号処理部１４０４が、秘密復号鍵Ｋｍｅｄｉａ（１）で復号処理することにより、セッションキーＫｓを復号し抽出する（ステップＳ１１４）。

【０３０９】

さらに、メモリカード１４０においては、Ｋｓ１発生部１４３２によりセッションキーＫｓ１が生成される（ステップＳ１１５）。

【０３１０】

続いて、配信モードにおいては、切換スイッチ１４０９は、接点ＰａまたはＰｂが順次閉じる状態が選択されるので、暗号化処理部１４０６は、接点Ｐａを介してセッションキー発生部１４３２から与えられるセッションキーＫｓ１と接点Ｐｂを介してＫＰｃａｒｄ（１）保持部１４０５から与えられる公開暗号化鍵ＫＰｃａｒｄ（１）（メモリカード１４０に対する公開暗号化鍵）とを、セッションキーＫｓにより暗号化し（ステップＳ１１６）、データ［ＫＰｃａｒｄ（１）、Ｋｓ１］Ｋｓを生成する（ステップＳ１１８）。

【０３１１】

携帯電話機１０５は、暗号化処理部１４０６により暗号化されたデータ［ＫＰｃａｒｄ（１）、Ｋｓ１］Ｋｓを配信サーバ１２に対して送信する（ステップＳ１２０）。

【０３１２】

配信サーバ１２では、通信装置３５０によりデータ［ＫＰｃａｒｄ（１）、Ｋｓ１］Ｋｓが受信され（ステップＳ１２２）、データバスＢＳ１に与えられたデータ［ＫＰｃａｒｄ（１）、Ｋｓ１］Ｋｓを復号処理部３１８が、セッションキーＫｓにより復号処理して、公開暗号化鍵ＫＰｃａｒｄ（１）およびセッションキーＫｓ１を復号抽出する（ステップＳ１２４）。

【０３１３】

続いて、配信制御部３１２は、配信情報データベース３０４等に保持されているデータを元に、ライセンスＩＤデータ等を含むライセンス情報データＬｉｃｅｎｓｅを生成する（ステップＳ１２６）。

【０３１４】

さらに、配信サーバ１２は、暗号化コンテンツデータ［Ｄｃ］Ｋｃを配信情報データベース３０４より取得して、通信装置３５０を介して、メモリカード１４０に送信する（ステップＳ１２８）。

【０３１５】

携帯電話機１０５が暗号化コンテンツデータ［Ｄｃ］Ｋｃを受信すると（ステップＳ１３０）、メモリカード１４０においては、受信した暗号化コンテンツデータ［Ｄｃ］Ｋｃをそのままメモリ１４１２に格納する（ステップＳ１３２）。

【０３１６】

一方、配信サーバ１２は、ライセンスキーＫｃを配信情報データベース３０４より取得し（ステップＳ１３４）、暗号化処理部３２０は、配信制御部３１２からのライセンスキーＫｃとライセンス情報データＬｉｃｅｎｓｅとを、復号処理部３１８より与えられた公開暗号化鍵ＫＰｃａｒｄ（１）により暗号化処理する（ステップＳ１３６）。

【０３１７】

暗号化処理部３２２は、暗号化処理部３２０により暗号化されたデータ［Ｋｃ、Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）を受取って、さらに、メモリカード１４０からのセッションキーＫｓ１により暗号化したデータをデータバスＢＳ１に与える。通信装置３５０は、暗号化処理部３２２により暗号化されたデータ［［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）］Ｋｓ１をメモリカード１４０に対して送信する。

【０３１８】

携帯電話機１０５がデータ［［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）］Ｋｓ１を受信すると（ステップＳ１４２）、メモリカード１４０においては、復号処理部１４１０が接点Ｐｆを介してＫｓ１発生部１４３２から与えられるセッションキーＫｓ１により復号処理を行ない、データ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）を抽出し、メモリ１４１２に格納する（ステップＳ１４６）。

【０３１９】

さらに、メモリカード１４０においては、コントローラ１４２０により制御されて、復号処理部１４１６が、メモリ１４１２に格納されたデータ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）を復号し、復号されたライセンス情報データＬｉｃｅｎｓｅを、レジスタ１５００に格納する（ステップ１４８）。

【０３２０】

以上のような動作により、メモリカード１４０自身が、暗号化コンテンツデータを送る側（配信サーバ１２）に、公開暗号化鍵ＫＰｍｅｄｉａ（１）およびセッションキーＫｓ１を送信した上で、配信を受けることができ、メモリカード１４０は、音楽を再生可能な状態となる。

【０３２１】

さらに、メモリカード１４０から配信サーバ１２へは、配信受理が通知され、配信サーバ１２で配信受理を受信すると（ステップＳ１５０）、課金データベース３０２にユーザ１の課金データが格納され（ステップＳ１５２）、処理が終了する（ステップＳ１５４）。

【０３２２】

以上のような配信モードでは、メモリカードおよび携帯電話機の認証がなされ

た上でコンテンツデータの配信が行われるので、システムのセキュリティおよび著作権の保護がより強化される。

【０３２３】

［再生モード］

図３７および図３８は、携帯電話機１０５内において、メモリカード１４０に保持された暗号化コンテンツデータから、音楽信号を復号化し、音楽として外部に出力するための再生処理を説明する第１および第２のフローチャートである。

【０３２４】

図３７および図３８を参照して、携帯電話機１０５のタッチキー１１０８等からのユーザ１の指示により、再生リクエストが携帯電話機１０５に対して出力される（ステップＳ２００）。

【０３２５】

これに応じて携帯電話機１０５からは、メモリカード１４０に対して、データ［ＫＰｐ，Ｃｒｔｆ（ｐ）］ＫＰｍａｓｔｅｒが送信される（ステップＳ２４１）。

【０３２６】

メモリカード１４０においては、データ［ＫＰｐ，Ｃｒｔｆ（ｐ）］ＫＰｍａｓｔｅｒを受信すると、復号処理部１４５２により復号処理が行われ、公開暗号化鍵ＫＰｐおよびデータＣｒｔｆの抽出が行われる（ステップＳ２４３）。

【０３２７】

抽出された証明データＣｒｔｆに基づいて、コントローラ１４２０は、携帯電話機１０５が正規の機器であるかを判断し（ステップＳ２４５）、正規の機器と判断した場合は、処理は次のステップＳ２４６に移行し、正規の機器でないと判断した場合は、処理を終了する（ステップＳ２８０）。

【０３２８】

正規の機器であると判断された場合、メモリカード１４０では、セッションキーＫｓ１を生成する（ステップＳ２４６）。メモリカード１４０は、さらに、抽出された公開暗号化鍵ＫＰｐによりセッションキーＫｓ１を暗号化し（ステップＳ２４８）、生成された暗号化セッションキー［Ｋｓ１］Ｋｐを携帯電話機１０

５に対して送信する（ステップＳ２５０）。

【０３２９】

携帯電話機１０５では、メモリカード１４０からの暗号化セッションキー［Ｋｓ１］Ｋｐを受信すると、復号処理部１５２２が、秘密復号鍵Ｋｐにより復号化してメモリカード１４０で生成したセッションキーＫｓ１を抽出する（ステップＳ２５２）。続いて、Ｋｓ発生部１５０２がセッションキーＫｓを生成し（ステップＳ２５３）、携帯電話機１０５の暗号化処理部１５０４は、携帯電話機１０５で生成したセッションキーＫｓをセッションキーＫｓ１により暗号化して、暗号化セッションキー［Ｋｓ］Ｋｓ１を生成し（ステップＳ２５４）、この暗号化セッションキー［Ｋｓ］Ｋｓ１をメモリカード１４０に対して送信する（ステップＳ２５６）。

【０３３０】

メモリカード１４０は、データバスＢＳ２を介して、携帯電話機１０５により生成され、かつ暗号化されたセッションキーＫｓを受け取り、セッションキーＫｓ１により復号し、携帯電話機１０５で生成したセッションキーＫｓを抽出する（ステップＳ２５８）。

【０３３１】

続いて、メモリカード１４０において、コントローラ１４２０は、レジスタ１５００に保持されるライセンス情報データＬｉｃｅｎｓｅに基づいて、復号可能であるかを判断し（ステップＳ２５９）、復号可能と判断した場合は、次の処理に移行し、復号不可能と判断した場合は、処理を終了する（ステップＳ２８０）。

【０３３２】

続いて、メモリカード１４０は、メモリ１４１２から、暗号化されているデータ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）を読み出し、復号処理部１４１６が復号処理を行なう（ステップＳ２６０）。

【０３３３】

秘密復号鍵Ｋｃａｒｄ（１）により、メモリ１４１２から読み出されたデータを復号可能な場合（ステップＳ２６２）、ライセンスキーＫｃが抽出される（ス

テップＳ２６４）。一方、復号不可能の場合、処理は終了する（ステップＳ２８０）。

【０３３４】

メモリ１４１２から読み出されたデータを復号可能な場合は、さらに、レジスタ１５００内のライセンス情報データＬｉｃｅｎｓｅのうち、再生回数に関するデータが変更される（ステップＳ２６６）。

【０３３５】

続いて、メモリカード１４０においては、暗号化処理部１４０６が、抽出したセッションキーＫｓにより、ライセンスキーＫｃを暗号化し（ステップＳ２６８）、暗号化されたライセンスキー［Ｋｃ］Ｋｓをデータバスｂｓ２に与える（ステップＳ２７０）。

【０３３６】

携帯電話機１０５の復号処理部１５０６は、セッションキーＫｓにより復号化処理を行なうことにより、ライセンスキーＫｃを取得する（ステップＳ２７２）。

【０３３７】

続いて、メモリカード１４０は、暗号化コンテンツデータ［Ｄｃ］Ｋｃをメモリ１４１２から読み出し、データバスｂｓ２に与える（ステップＳ２７４）。

【０３３８】

携帯電話機１０５の音楽再生部１５０８は、暗号化コンテンツデータ［Ｄｃ］Ｋｃを、抽出されたライセンスキーＫｃにより復号処理して平文のコンテンツデータを生成し（ステップＳ２７６）、コンテンツデータから音楽信号を再生して混合部１５１０に与える（ステップＳ２７６）。デジタルアナログ変換部１５１２は、混合部１５１０からのデータを受け取って変換し、外部に再生された音楽を出力し、処理が終了する（ステップＳ２３２）。

【０３３９】

このような構成とすることで、メモリカード自身および携帯電話自身が、それぞれセッションキーＫｓ１またはＫｓを生成し、これにより暗号化コンテンツデータの授受を行なった上で、再生動作を行なうことが可能となる。

【０３４０】

さらに、メモリカード１４０が携帯電話機１０５の認証を行なった上で、再生動作を行なうため、システムのセキュリティおよび著作権の保護が向上する。

【０３４１】

［移動または複製モード］

図３９および図４０は、２つのメモリカード間において、コンテンツデータおよびキーデータ等の移動または複製を行なう処理を説明するための第１および第２のフローチャートである。

【０３４２】

まず、携帯電話機１０５と同様の構成を有する携帯電話機１０６が送信側であり、携帯電話機１０５が受信側であるものとする。また、携帯電話機１０６にも、メモリカード１４０と同様の構成を有するメモリカード１４２が装着されているものとする。

【０３４３】

携帯電話機１０６は、まず、携帯電話機１０５に対して、移動リクエストまたは複製リクエストを出力する（ステップＳ３００）。

【０３４４】

携帯電話機１０５がこのリクエストを受信すると（ステップＳ３０１）、メモリカード１４２は、これに応じて、メモリ１４１２内の暗号化コンテンツデータ［Ｄｃ］Ｋｃを読み出して、メモリカード１４０に対して出力し（ステップＳ３０２）、メモリカード１４０では、暗号化コンテンツデータ［Ｄｃ］Ｋｃをメモリ１４１２に格納する（ステップＳ３０４）。

【０３４５】

続いて、携帯電話機１０６および１０５においては、ステップＳ３００において与えられたリクエストが、「移動リクエスト」であるか「複製リクエスト」であるかが判断され（ステップＳ３０６、ステップＳ３０６′）、「移動リクエスト」である場合、メモリカード１４０は、この移動リクエストに応じて、［ＫＰｍｅｄｉａ，Ｃｒｔｆ］ＫＰｍａｓｔｅｒ保持部１４４２から、公開暗号化鍵ＫＰｍｅｄｉａ（１）および証明データＣｒｔｆ（１）を暗号化したデータ［ＫＰ

ｍｅｄｉａ（１），Ｃｒｔｆ（１）］ＫＰｍａｓｔｅｒを携帯電話機１０５に対して出力する（ステップＳ３０７）。

【０３４６】

携帯電話機１０５では、メモリカード１４０からのデータ［ＫＰｍｅｄｉａ（１），Ｃｒｔｆ（１）］ＫＰｍａｓｔｅｒを携帯電話機１０６に対して送信する（ステップＳ３０８）。

【０３４７】

携帯電話機１０６では、メモリカード１４０から転送されたデータ［ＫＰｍｅｄｉａ（１），Ｃｒｔｆ（１）］ＫＰｍａｓｔｅｒを受信すると（ステップＳ３０９）、メモリカード１４２内の復号処理部１４５２が復号処理を行い、証明データＣｒｔｆ（１）、公開暗号化鍵ＫＰｍｅｄｉａ（１）の抽出を行なう（ステップＳ３１０）。

【０３４８】

復号された証明データＣｒｔｆ（１）に基づいて、コントローラ１４２０は、認証を行ない、正規メモリカードからのアクセスの場合は次の処理に移行し（ステップＳ３１１）、正規メモリカードでない場合には、携帯電話機１０６は移動不可の通知を送信するとともに、メモリカード１４２は処理を終了する（ステップＳ３７４）。携帯電話機１０５が移動不可通知を受信すると（ステップＳ３１３）、メモリカード１４０も処理を終了する（ステップＳ３７４）。

【０３４９】

一方、ステップＳ３１１での照会の結果、正規メモリカードであることが確認されると、メモリカード１４２のＫｓ２発生回路１４３２は、セッションキーＫｓ２を生成し（ステップＳ３１４）、公開暗号化鍵ＫＰｍｅｄｉａ（１）を用いて、暗号化処理部１４３０がセッションキーＫｓ２を暗号化する（ステップＳ３１５）。

【０３５０】

携帯電話機１０６は、暗号化セッションキー［Ｋｓ２］ＫＰｍｅｄｉａ（１）を携帯電話機１０５に対して送信する（ステップＳ３１６）。携帯電話機１０５は、暗号化セッションキー［Ｋｓ２］ＫＰｍｅｄｉａ（１）を受信すると（ステ

ップＳ３１８）、メモリカード１４０に伝達し、メモリカード１４０は、復号処理部１４０４が復号して、セッションキーＫｓ２を受理する（ステップＳ３２０）。さらに、メモリカード１４０においてセッションキーＫｓ１が生成される（ステップＳ３２１）。

【０３５１】

メモリカード１４０においては、セッションキーＫｓ２によりメモリカード１４０の公開暗号化鍵ＫＰｃａｒｄ（１）およびセッションキーＫｓ１を暗号化して（ステップＳ３２２）、携帯電話機１０５から携帯電話機１０６に対して暗号化されたデータ［ＫＰｃａｒｄ（１）、Ｋｓ１］Ｋｓ２を送信する（ステップＳ３２４）。携帯電話機１０６は、データ［ＫＰｃａｒｄ（１）、Ｋｓ１］Ｋｓ２を受信し（ステップＳ３２６）、メモリカード１４２に転送する。

【０３５２】

メモリカード１４２においては、復号処理部１４１０が、メモリカード１４０から送信された暗号化データ［ＫＰｃａｒｄ（１）、Ｋｓ１］Ｋｓ２をセッションキーＫｓ２により復号化して、メモリカード１４０の公開暗号化鍵ＫＰｃａｒｄ（１）、セッションキーＫｓ１を復号抽出する（ステップＳ３３０）。

【０３５３】

続いて、メモリカード１４２においては、メモリ１４１２からメモリカード１４２の公開暗号化鍵ＫＰｃａｒｄ（２）により暗号化されているライセンスキーＫｃ、ライセンス情報データＬｉｃｅｎｓｅに対応する［Ｋｃ、Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（２）読出される（ステップＳ３３２）。

【０３５４】

続いて、メモリカード１４２の復号処理部１４１６が、秘密復号鍵Ｋｃａｒｄ（２）により、ライセンスキーＫｃ、ライセンス情報データＬｉｃｅｎｓｅを復号処理する（ステップＳ３３４）。

【０３５５】

メモリカード１４２のコントローラ１４２０は、このようにして復号されたライセンス情報データＬｉｃｅｎｓｅの値を、レジスタ１５００内のデータ値と置換する（ステップＳ３３６）。

【０３５６】

さらに、メモリカード１４２の暗号化処理部１４１４は、復号処理部１４１０において抽出されたメモリカード１４０における公開暗号化鍵ＫＰｃａｒｄ（１）により、ライセンスキーＫｃ、ライセンス情報データＬｉｃｅｎｓｅとを暗号化する（ステップＳ３３８）。

【０３５７】

メモリカード１４２の暗号化処理部１４１４により暗号化されたデータは、切換スイッチ１４０９（接点Ｐｄが閉じている）を介して、さらに、暗号化処理部１４０６に与えられ、メモリカード１４２の暗号化処理部１４０６は、データ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）をセッションキーＫｓ１により暗号化してデータ［［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）］Ｋｓ１を生成する（ステップＳ３４０）。

【０３５８】

続いて、メモリカード１４２は、携帯電話機１０６に対してデータ［［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）］Ｋｓ１を出力し（ステップＳ３４２）、携帯電話機１０６はデータ［［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）］Ｋｓ１を携帯電話機１０５に対して送信する（ステップＳ３４４）。

【０３５９】

携帯電話機１０５が受信したデータ［［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）］Ｋｓ１は（ステップＳ３４６）、メモリカード１４０に対して伝達され、メモリカード１４０の復号処理部１４１０は、暗号化されたデータ［［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）］Ｋｓ１を復号して、データ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）を受理する（ステップＳ３４８）。

【０３６０】

メモリカード１４０においては、復号処理部１４１０により、セッションキーＫｓ１に基づいて復号化処理されたデータ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）をメモリ１４１２に格納する（ステップＳ３５０）。さらに、メモリカード１４０においては、復号処理部１４１６が、秘密復号鍵Ｋｃａｒｄ（１）に基づいて、データ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）を復号し、復号され

たライセンス情報データＬｉｃｅｎｓｅをレジスタ１５００に格納する（ステップＳ３５２）。

【０３６１】

以後の移動モードにおける処理ならびに複製モードにおけるメモリカード１４０および１４２の処理は、図１８および図１９で説明した実施の形態２のメモリカード１２０、１２２等の処理と同様であるので、その説明は繰り返さない。

【０３６２】

このような構成とすることで、移動元および移動先のメモリカード自身が、セッションキーをそれぞれ生成した上で、移動動作を行なうこと、および複製動作を行なうことが可能となる。

【０３６３】

したがって、データバス上等で伝達されるデータの暗号化キーが、セッションごとに、かつ、機器ごとに変更されるので、データ授受のセキュリティが一層向上するという効果がある。

【０３６４】

しかも、以上のような構成を用いることで、たとえば、メモリカード１４２からメモリカード１４０へのデータの移動を、上述したようなセッションキー発生回路１５０２を有する携帯電話端末を介さずに、メモリカードとメモリカードとを接続可能なインターフェース機器により行なうことも可能となり、ユーザの利便性が一層向上するという効果がある。

【０３６５】

ここで、移動モード時には、再生情報内の再生回数を制限するライセンス情報データについては、メモリ１４１２に記録されたライセンス情報データを、レジスタ１５００にて再生の都度修正された再生回数を記録したライセンス情報データに変更することでライセンス情報データを更新する。このようにして、メモリカード間をコンテンツデータが移動しても、再生回数に制限があるコンテンツデータの再生回数は、配信時に決められた再生回数の制限を越えることがないようにすることが可能である。

【０３６６】

しかも、メモリカード１４２がメモリカード１４０の認証を行った上で、移動動作を行なうため、システムのセキュリティおよび著作権の保護が向上する。

【０３６７】

［実施の形態６］

図４１は、本発明の実施の形態６のコンテンツデータ販売機３０１０の構成を示す概略ブロック図であり、実施の形態４の図２７と対比される図である。

【０３６８】

ただし、以下の説明では、実施の形態５で説明したメモリカード１４０との間のインターフェースのためにメモリスロット２０３０を設ける構成とし、実施の形態４の変形例と同様に、携帯電話機１０５を介することなく、メモリカード１４０とコンテンツデータ販売機３０１０とが直接データの授受を行なう構成であるものとする。

【０３６９】

もちろん、コネクタ２０１０により、携帯電話機１０５を介して、メモリカード１４０とコンテンツデータ販売機３０１０とがデータの授受を行なう構成とすることも可能である。

【０３７０】

したがって、コンテンツデータ販売機３０１０の構成が、実施の形態４のコンテンツデータ販売機３０００の構成と異なる点は、コネクタ２０１０の代わりに、メモリスロット２０３０が設けられていることと、データ処理部２１００は、公開復号鍵ＫＰｍａｓｔｅｒを保持するＫＰｍａｓｔｅｒ保持部３２４と、ＫＰｍａｓｔｅｒ保持部３２４から出力される公開復号鍵ＫＰｍａｓｔｅｒに基づいて、通信網から通信装置３５０を介してデータバスＢＳ１に与えられるデータを復号するための復号処理部３２６とをさらに備える構成となっている点である。暗号化処理部３１６は、復号処理部３２６での復号処理により抽出された公開暗号化鍵ＫＰｍｅｄｉａにより、Ｋｓ発生部３１４で発生されたセッションキーＫｓを暗号化し、また、配信制御部３１２は、復号処理部３２６での復号処理により抽出された証明データＣｒｔｆにより、配信を求めてきたメモリカードが正規のメモリカードであるかの認証を行なう。

【０３７１】

コンテンツデータ販売機３０１０のその他の点は、図２７に示した実施の形態４のコンテンツデータ販売機３０００の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

【０３７２】

［配信モード］

図４２および図４３は、図４１で説明したコンテンツデータ販売機３０１０を用いたデータ配信システムにおける配信動作を説明するための第１および第２のフローチャートである。

【０３７３】

図４２および図４３においては、ユーザ１が、メモリカード１４０を用いることで、コンテンツデータ販売機３０１０からコンテンツデータ（音楽データ）の配信を受ける場合の動作を説明している。

【０３７４】

まず、ユーザが、コンテンツデータ販売機３０１０のキーボード２００４のキーボタンの操作等によって、配信リクエストを指示する（ステップＳ５００）。

【０３７５】

コンテンツデータ販売機３０１０からは、メモリカード１４０に対して、認証のためのデータ［ＫＰｍｅｄｉａ，Ｃｒｔｆ］ＫＰｍａｓｔｅｒの送信依頼が出力される（ステップＳ５０２′）。

【０３７６】

メモリカード１４０においては、この送信依頼に応じて、［ＫＰｍｅｄｉａ，Ｃｒｔｆ］ＫＰｍａｓｔｅｒ保持部１４４２から、公開暗号化鍵ＫＰｍｅｄｉａ（１）および証明データＣｒｔｆ（１）を暗号化したデータ［ＫＰｍｅｄｉａ（１），Ｃｒｔｆ（１）］ＫＰｍａｓｔｅｒをコンテンツデータ販売機３０１０に対して出力する（ステップＳ５０７）。

【０３７７】

コンテンツデータ販売機３０１０では、メモリカード１４０から転送されたデータ［ＫＰｍｅｄｉａ（１），Ｃｒｔｆ（１）］ＫＰｍａｓｔｅｒを受信すると

、公開復号鍵ＫＰｍａｓｔｅｒにより復号処理部３２６が復号処理を行い、証明データＣｒｔｆ（１）、公開暗号化鍵ＫＰｐ、公開暗号化鍵ＫＰｍｅｄｉａ（１）の抽出を行なう（ステップＳ５０９）。

【０３７８】

復号された証明データＣｒｔｆ（１）に基づいて、配信制御部３１２は、正規メモリカードからのアクセスかどうかの判断を行なう。正規のメモリカードの場合は次の処理に移行し（ステップＳ５１１）、正規メモリカードでない場合には、管理サーバ２２００中の管理データベースに異常終了記録を格納し（ステップＳ５６１）、処理を終了する（ステップＳ５６２）。

【０３７９】

コンテンツデータ販売機３０１０は、ステップＳ５１１での照会の結果、正規メモリカードであることが確認されると、ディスプレイ２００２を介してユーザに料金投入を案内し、料金徴収を行なう（ステップＳ５１２）。

【０３８０】

続いて、コンテンツデータ販売機３０１０は、セッションキー発生部３１４が、セッションキーＫｓを生成する。さらに、コンテンツデータ販売機３０１０内の暗号化処理部３１６が、受信した公開暗号化鍵ＫＰｍｅｄｉａ（１）により、このセッションキーＫｓを暗号化して暗号化セッションキー［Ｋｓ］Ｋｍｅｄｉａ（１）を生成する（ステップＳ５１４）。

【０３８１】

続いて、コンテンツデータ販売機３０１０は、暗号化セッションキー［Ｋｓ］Ｋｍｅｄｉａ（１）をデータバスＢＳ１に与え、カードスロット２０３０から出力する（ステップＳ５１６）。

【０３８２】

メモリカード１４０においては、メモリインタフェース１２００を介して、データバスＢＳ３に与えられた暗号化セッションキー［Ｋｓ］Ｋｍｅｄｉａ（１）を、復号処理部１４０４が、秘密復号鍵Ｋｍｅｄｉａ（１）により復号処理することにより、セッションキーＫｓを復号し抽出する（ステップＳ５２０）。さらに、メモリカード１４０では、セッションキーＫｓ１が生成される（ステップＳ

５２１）。

【０３８３】

続いて、配信モードにおいては、切換スイッチ１４０８は、接点Ｐａが閉じる状態が選択されているので、暗号化処理部１４０６は、接点Ｐａを介してＫＰｃａｒｄ（１）保持部１４０５から与えられる公開暗号化鍵ＫＰｃａｒｄ（１）を、セッションキーＫｓにより暗号化し（ステップＳ５２２）、データ［ＫＰｃａｒｄ（１）］Ｋｓを生成する（ステップＳ５２４）。

【０３８４】

コンテンツデータ販売機３０１０では、カードスロット２０３０を介してデータ［ＫＰｃａｒｄ（１）］Ｋｓが受信され（ステップＳ５２８）、データバスＢＳ１に与えられたデータ［ＫＰｃａｒｄ（１）］Ｋｓを復号処理部３１８が、セッションキーＫｓにより復号処理して、公開暗号化鍵ＫＰｃａｒｄ（１）を復号抽出する（ステップＳ５３０）。

【０３８５】

続いて、配信制御部３１２は、配信情報データベース３０４等に保持されているデータを元に、ライセンスＩＤデータ等を含むライセンス情報データＬｉｃｅｎｓｅを生成する（ステップＳ５３２）。

【０３８６】

さらに、コンテンツデータ販売機３０１０は、暗号化コンテンツデータ［Ｄｃ］Ｋｃを配信情報データベース３０４より取得して、カードスロット２０３０を介して、メモリカード１４０に送信する（ステップＳ５３４）。

【０３８７】

メモリカード１４０においては、受信した暗号化コンテンツデータ［Ｄｃ］Ｋｃをそのままメモリ１４１２に格納する（ステップＳ５３８）。

【０３８８】

一方、コンテンツデータ販売機３０１０は、ライセンスキーＫｃを配信情報データベース３０４より取得し（ステップＳ５４０）、暗号化処理部３２０は、配信制御部３１２からのライセンスキーＫｃとライセンス情報データＬｉｃｅｎｓｅとを、復号処理部３１８より与えられた公開暗号化鍵ＫＰｃａｒｄ（１）によ

り暗号化処理する（ステップＳ５４２）。

【０３８９】

暗号化処理部３２２は、暗号化処理部３２０により暗号化されたデータ［Ｋｃ、Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）を受取って、さらにセッションキーＫｓにより暗号化したデータをデータバスＢＳ１に与え、暗号化処理部３２２により暗号化されたデータ［［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）］Ｋｓ１がメモリカード１４０に対して送信される（ステップＳ５４６）。

【０３９０】

メモリカード１４０においては、復号処理部１４１０がセッションキーＫｓ１により復号処理を行ない、データ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）を抽出し、メモリ１４１２に格納する（ステップＳ５５２）。

【０３９１】

さらに、メモリカード１４０においては、コントローラ１４２０により制御されて、復号処理部１４１６が、メモリ１４１２に格納されたデータ［Ｋｃ，Ｌｉｃｅｎｓｅ］Ｋｃａｒｄ（１）を復号し、復号されたライセンス情報データＬｉｃｅｎｓｅを、レジスタ１５００に格納する（ステップＳ５５４）。

【０３９２】

以上のような動作により、メモリカード１４０は、コンテンツデータから音楽を再生可能な状態となる。

【０３９３】

さらに、メモリカード１４０からコンテンツデータ販売機３０１０へは、配信受理が通知され（ステップＳ５５８）、コンテンツデータ販売機３０１０で配信受理を受信すると、管理サーバ２２００中の管理データベースに販売記録が送信され（ステップＳ５６０）、処理が終了する（ステップＳ５６２）。

【０３９４】

以上のような構成により、ユーザは、より簡易に暗号化された音楽データ等のコンテンツデータの配信を受けることができる。しかも、メモリカードの認証がなされた上でコンテンツデータの配信が行われるので、システムのセキュリティおよび著作権の保護がより強化される。

【０３９５】

［実施の形態７］

図４４は、実施の形態７における携帯電話機１０７の構成を説明するための概略ブロック図である。

【０３９６】

図３２に示した実施の形態５の携帯電話機１０５の構成と異なる点は、携帯電話機という再生装置に共通な復号鍵Ｋｃｏｍを保持するＫｃｏｍ保持部１５３０と、復号処理部１５０６の出力を受けて、復号鍵Ｋｃｏｍについて復号し、音楽再生部１５０８にライセンスキーＫｃを与える復号処理部１５３２とを備える構成となっていることである。

【０３９７】

携帯電話機１０７のその他の点は、図３２に示した実施の形態５の携帯電話機１０５の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。メモリカード１４０の構成も同様である。

【０３９８】

すなわち、実施の形態７では、実施の形態５において、音楽再生部１５０８に最終的にライセンスキーＫｃと与えられる以前において、システムを構成する機器間で授受されていたライセンスキーＫｃを、実施の形態７では、さらに暗号化した［Ｋｃ］Ｋｃｏｍという状態でやり取りする以外は、実施の形態５の構成と同様である。

【０３９９】

なお、以下の説明では、復号鍵Ｋｃｏｍは共通鍵であるものとして説明するが、本発明はこのような場合に限定されず、たとえば、暗号化は公開鍵ＫＰｃｏｍで行い、復号化を公開暗号化鍵ＫＰｃｏｍとは非対称な秘密復号鍵Ｋｃｏｍで行なう構成としてもよい。

【０４００】

図４５は、実施の形態７の携帯電話機１０７に対応した配信サーバ１３の構成を示す概略ブロック図である。図３３に示した実施の形態５の配信サーバ１２の構成と異なる点は、データ処理部３１０は、復号鍵Ｋｃｏｍを保持するＫｃｏｍ

保持部３３０と、配信制御部３１２を介して配信情報データベース３０４から与えられるライセンスキーＫｃを復号鍵Ｋｃｏｍにより暗号化処理して、暗号化ライセンスキー［Ｋｃ］Ｋｃｏｍとして暗号化処理部３２０に与える暗号化処理部３３２をさらに備える構成となっている点である。

【０４０１】

配信サーバ１３のその他の点は、図３３に示した実施の形態５の配信サーバ１２の構成の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

【０４０２】

［配信モード］

図４６および図４７は、図４４および４５で説明した配信サーバ１３と携帯電話機１０７を用いた配信モードを説明するための第１および第２のフローチャートである。

【０４０３】

図４６および図４７においても、ユーザ１が、メモリカード１４０を用いることで、配信サーバ１３からコンテンツデータ（音楽データ）の配信を受ける場合の動作を説明している。

【０４０４】

ただし、図４６および図４７の処理は、ステップＳ１３４において、配信サーバ１３が、ライセンスキーＫｃを配信情報データベース３０４より取得した後、暗号化処理部３３２がキーＫｃを暗号化して（ステップＳ１３５）、以後は、暗号化ライセンスキー［Ｋｃ］Ｋｃｏｍとして授受される点を除いては、図３５および図３６で説明した実施の形態５の配信モードと同様であるので、その説明は繰り返さない。

【０４０５】

以上のような配信モードでは、実施の形態５に比べて、さらにシステムのセキュリティが強化される。

【０４０６】

［再生動作］

図４８および図４９は、携帯電話機１０７内において、メモリカード１４０に保持された暗号化コンテンツデータから、音楽信号を再生し、音楽として外部に出力するための再生処理を説明する第１および第２のフローチャートである。

【０４０７】

ただし、図４８および図４９に示した再生処理は、ステップＳ２６４でメモリカード１４０のメモリ１４１２から読み出されるキーが、暗号化ライセンスキー［Ｋｃ］Ｋｃｏｍであり、以後、暗号化ラセンスキー［Ｋｃ］Ｋｃｏｍとして携帯電話機１０７に送信され、携帯電話機１０７において、ステップＳ２７３で復号処理部１５３２によりキー［Ｋｃ］Ｋｃｏｍが復号されライセンスキーＫｃが音楽再生部１５０８に与えられる点以外は、図３７および図３８に示した実施の形態５の再生処理と同様であるのでその説明は繰り返さない。

【０４０８】

このような構成とすることで、再生モードにおけるシステムのセキュリティおよび著作権の保護が一層向上する。

【０４０９】

［移動または複製モード］

図５０および図５１は、実施の形態７において、２つのメモリカード間において、コンテンツデータおよびキーデータ等の移動または複製を行なう処理を説明するための第１および第２のフローチャートである。

【０４１０】

ただし、図５０および図５１の処理は、ライセンスキーＫｃが、暗号化ライセンスキー［Ｋｃ］Ｋｃｏｍとして授受される点を除いては、図３９および図４０で説明した実施の形態５の移動または複製モードの動作と同様であるので、その説明は繰り返さない。

【０４１１】

このような構成とすることで、移動または複製モードにおけるシステムのセキュリティおよび著作権の保護が一層向上する。

【０４１２】

［実施の形態８］

図５２は、本発明の実施の形態８のコンテンツデータ販売機３０２０の構成を示す概略ブロック図であり、実施の形態６の図４１と対比される図である。

【０４１３】

コンテンツデータ販売機３０２０の構成が、実施の形態６のコンテンツデータ販売機３０１０の構成と異なる点は、データ処理部２１００は、復号鍵Ｋｃｏｍを保持するＫｃｏｍ保持部３３０と、配信制御部３１２を介して配信情報データベース３０４から与えられるライセンスキーＫｃを復号鍵Ｋｃｏｍにより暗号化処理して、暗号化ライセンスキー［Ｋｃ］Ｋｃｏｍとして暗号化処理部３２０に与える暗号化処理部３３２をさらに備える構成となっている点である。

【０４１４】

コンテンツデータ販売機３０２０のその他の点は、図４１に示した実施の形態６のコンテンツデータ販売機３０１０の構成の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

【０４１５】

もちろん、実施の形態８でも、コネクタ２０１０により、携帯電話機１０７を介して、メモリカード１４０とコンテンツデータ販売機３０２０とがデータの授受を行なう構成とすることも可能である。

【０４１６】

［配信モード］

図５３および図５４は、図５２で説明したコンテンツデータ販売機３０２０を用いたデータ配信システムにおける配信モードを説明するための第１および第２のフローチャートである。

【０４１７】

図５３および図５４においては、ユーザ１が、メモリカード１４０を用いることで、コンテンツデータ販売機３０２０からコンテンツデータ（音楽データ）の配信を受ける場合の動作を説明している。

【０４１８】

ただし、図５３および図５４の処理は、ステップＳ５４０において、コンテンツデータ販売機３０２０が、ライセンスキーＫｃを配信情報データベース３０４

より取得した後、暗号化処理部３３２がライセンスキーＫｃを暗号化して（ステップＳ５４１）、以後は、暗号化ライセンスキー［Ｋｃ］Ｋｃｏｍとして授受される点を除いては、図４２および図４３で説明した実施の形態５の配信動作と同様であるので、その説明は繰り返さない。

【０４１９】

以上のような配信モードでは、実施の形態６に比べて、さらにシステムのセキュリティが強化される。

【０４２０】

ここでは暗号化コンテンツデータを配信し、メモリカード１１０、１２０、１４０内のメモリ１４１２に格納した後、ライセンスキーＫｃ、ライセンス情報データＬｉｃｅｎｓｅの配信を受けるように説明したが、逆にライセンスキーＫｃ、ライセンス情報データＬｉｃｅｎｓｅを配信し、メモリカード１１０、１２０、１４０内のレジスタ１５００に格納した後、暗号化コンテンツデータの配信を受けても構わない。

【０４２１】

さらに、移動モードにおいても配信モードと同様に、暗号化コンテンツデータ、ライセンスキーＫｃ、ライセンス情報データＬｉｃｅｎｓｅのいずれの移動が先であっても構わない。

【０４２２】

なお、以上説明してきた各実施の形態において、配信データとしてコンテンツデータに付随する非暗号化データ、たとえば、上記音楽データの曲名、実演者（歌手、演奏家等）、作曲家、作詞家等の当該音楽データ（コンテンツデータ）に関する著作情報や配信サーバ１０、１１、コンテンツデータ販売機３０００、３００１に対してアクセスするための情報等を、付加データＤｉとして暗号化コンテンツデータと併せて配信することも可能である。この付加データＤｉは、配信、移動、複製においてはコンテンツデータとともに処理され、再生時には分離されてコンテンツデータとは個別にアクセス可能となるように、暗号化コンテンツデータと同じメモリ１４１２に格納される。

【０４２３】

［実施の形態９］

図５５は、以上説明してきたメモリカード１１０，１２０，１４０等の端子１２０２部分の構成を説明する概略ブロック図である。

【０４２４】

以下では、メモリカード１４０の端子１２０２部分の構成であるものとして説明する。

【０４２５】

メモリカード１４０には、端子１２０２からシリアルにデータやコマンドが与えられる。これに対して、メモリカード１４０中のデータバスＢＳ３には、パラレルにデータやコマンドが伝達されるものとする。

【０４２６】

図５５は、このようなメモリカード１４０へのデータ入力時のシリアル・パラレル変換と、データ出力時のパラレル・シリアル変換を行なう構成を示す概略ブロック図である。

【０４２７】

端子１２０２中のデータピン１４６０には、データ入出力のタイミングを指定するための信号である信号ＣＳが与えられる。たとえば、信号ＣＳが活性化（“Ｌ”レベル）となった後の所定期間後に、データ入力ピン１４６２に与えられるデータが“Ｌ”レベルとなることで、データ入力のタイミングが検出される。どうように、信号ＣＳが活性化（“Ｌ”レベル）となった後の所定期間後に、データ出力ピン１４６４に出力されるデータが“Ｌ”レベルとなることで、データ出力のタイミングが検出される。インターフェースコントローラ１４９０は、メモリカード１４０の外部からデータバスＢＳ３へのデータ入力、およびデータバスＢＳ３からメモリカード１４０外部へのデータ出力を管理する。

【０４２８】

データ入力時は、データ入力ピン１４６２に与えられたデータは、バッファ１４６８を介して、縦列に接続されたＤ－フリップフロップ１４７０．０～１４７０．７に入力される。すなわち、８ビット分のデータが入力された時点で、Ｄ－フリップフロップ１４７０．０～１４７０．７の全てのデータが更新され、その

時点で、インターフェースコントローラ１４９０により制御されて、データバッファ１４２７．０～１４２７．７からデータバスＢＳ３へデータがパラレルに出力される。

【０４２９】

データ出力時は、データバスＢＳ３からのデータがマルチプレクサ１４７６．１～１４７６．７を介して、パラレルに与えられＤ－フリップフロップ１４７４．０～１４７４．７に格納される。その後インターフェースコントローラ１４９０により制御されて、マルチプレクサ１４７６．１～１４７６．７の接続が切換わり、Ｄ－フリップフロップ１４７４．０～１４７４．７が縦列に接続される。この状態で、Ｄ－フリップフロップ１４７４．０～１４７４．７のそれぞれに格納されたデータが、順次シリアルに、インターフェースコントローラ１４９０により制御される出力バッファ１４７０を介して、データ出力ピン１４６４から出力される。

【０４３０】

［実施の形態９の変形例］

図５６は、データ入力の速度を向上させるために、データ入力ピンの本数を１本から２本または４本に可変とすることが可能な、メモリカード１４０の端子１２０２部分の構成の変形例を説明するための概略ブロック図である。

【０４３１】

図５５に示した構成と異なる点は、まず、４本のデータ入力ピン１４６２．０～１４６２．３およびそれらに対応する入力バッファ１４６８．０～１４６８．３が設けられていることと、これらデータ入力ピン１４６２．０～１４６２．３に与えらたコマンドを入力バッファ１４６８．０～１４６８．３からインターフェースコントローラ１４９０に伝達するためのマルチプレクサ１４６７と、データ入力ピン１４６２．０～１４６２．３に与えらたデータまたはコマンドを、入力バッファ１４６８．０～１４６８．３からＤ－フリップフロップ１４７０．０～１４７０．７に選択的に与えるためのマルチプレクサ１４６９．１～１４６９．７とをさらに備える構成となっていることである。

【０４３２】

次に動作について簡単に説明する。

電源投入後には、たとえば、メモリカード１４０は、１本のデータ入力ピン１４６２．０からのみデータ入力を受けつける状態となっている。

【０４３３】

以下では、外部からデータ入力ピン１４６２．０～１４６２．３およびマルチプレクサ１４６７を経由してインターフェースコントローラ１４９０に与えらたコマンドにより、インターフェースコントローラ１４９０がマルチプレクサ１４６９．１～１４６９．７を制御することで、４本のデータ入力ピン１４６２．０～１４６２．３からのデータをパラレルに入力するモードに動作モードが変更されたものとする。

【０４３４】

まず、第１のタイミングで４本のデータ入力ピン１４６２．０～１４６２．３に与えられたデータは、マルチプレクサ１４６９．１～１４６９．３を経由してＤ－フリップフロップ１４７０．０～１４７０．３に与えられる。

【０４３５】

次の第２のタイミングで、マルチプレクサ１４６９．１～１４６９．７の接続が切換わり、Ｄ－フリップフロップ１４７０．０～１４７０．３の出力がそれぞれ、Ｄ－フリップフロップ１４７０．４～１４７０．７に与えられて格納される。さらに第３のタイミングで、４本のデータ入力ピン１４６２．０～１４６２．３に与えられたデータは、マルチプレクサ１４６９．１～１４６９．３を経由してＤ－フリップフロップ１４７０．０～１４７０．３に与えられる。

【０４３６】

以上で、８ビット分のデータのＤ－フリップフロップ１４７０．０～１４７０．７への格納が終了する。以後は、図５５の場合と同様に、データバスＢＳ３に対してパラレルに８ビット分のデータが与えられる。

【０４３７】

データ出力の際の動作は、図５５の場合と同様である。

以上のような構成により、データ配信時、特にコンテンツデータ販売機２０００等からコンテンツデータを購入する際のメモリカード１４０へのデータ配信時

間を短縮することが可能である。

【０４３８】

また、以上説明した各実施の形態のうち、２つの携帯電話にそれぞれ装着された２つのメモリカード間で、たとえば、ＰＨＳのトランシーバモード等を利用することにより、コンテンツデータの移動を行なう処理を説明した実施の形態においては、このような構成に限定されず、たとえば、１つの携帯電話機に複数のメモリカードが同時装着可能な場合は、当該携帯電話機に２つのメモリカードを同時に装着することで、コンテンツデータの移動を行なう構成とすることも可能である。このようなコンテンツデータの移動の場合は、以上説明した各実施の形態において、２つの携帯電話機間での送受信のやりとりを省略すればよい。

【０４３９】

今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は上記した説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

【０４４０】

【発明の効果】

以上説明したとおり、本願発明にかかる配信システムでは、正規のユーザのみがコンテンツデータを受信してメモリ中に格納することが可能となり、かつ、１度メモリカード中に格納されたデータを、他人にコピーさせる場合は、当該他人が再生可能な状態でデータを移植するためには、送信元においては、データの再生が不能となってしまう構成となっているので、無制限なコピーにより著作権が不当な不利益を被るのを防止することが可能となる。

【０４４１】

また、ユーザが配信キャリアを介してではなく、コンテンツデータ販売機により暗号化コンテンツデータを購入することができるので、ユーザの利便性が一層向上する。

【図面の簡単な説明】

【図１】　本発明の情報配信システムの全体構成を概略的に説明するための

概念図である。

【図２】　図１に示した情報配信システムにおいて使用される通信のためのキーデータ（鍵データ）等の特性をまとめて説明する図である。

【図３】　図１に示した配信サーバ１０の構成を示す概略ブロック図である。

【図４】　図１に示した携帯電話機１００の構成を説明するための概略ブロック図である。

【図５】　図４に示したメモリカード１１０の構成を説明するための概略ブロック図である。

【図６】　図１および図３～図５で説明したデータ配信システムにおける配信モードを説明するための第１のフローチャートである。

【図７】　図１および図３～図５で説明したデータ配信システムにおける配信モードを説明するための第２のフローチャートである。

【図８】　携帯電話機１００内においてコンテンツデータを再生し、、音楽として外部に出力するための再生処理を説明するフローチャートである。

【図９】　２つのメモリカード間において、コンテンツデータおよびキーデータ等の移動または複製を行なう処理を説明するための第１のフローチャートである。

【図１０】　２つのメモリカード間において、コンテンツデータおよびキーデータ等の移動または複製を行なう処理を説明するための第２のフローチャートである。

【図１１】　実施の形態２のメモリカード１２０に対応した音楽サーバ３１の構成を示す概略ブロック図である。

【図１２】　実施の形態２における携帯電話機１０１の構成を説明するための概略ブロック図である。

【図１３】　本発明の実施の形態２のメモリカード１２０の構成を説明するための概略ブロック図である。

【図１４】　図１３で説明したメモリカード１２０を用いた配信モードを説明するための第１のフローチャートである。

【図１５】　図１３で説明したメモリカード１２０を用いた配信モードを説明するための第２のフローチャートである。

【図１６】　携帯電話機１０１内においてコンテンツデータを再生し、音楽として外部に出力するための再生処理を説明する第１のフローチャートである。

【図１７】　携帯電話機１０１内においてコンテンツデータを再生し、音楽として外部に出力するための再生処理を説明する第２のフローチャートである。

【図１８】　２つのメモリカード間でコンテンツデータおよびキーデータ等の移動または複製を行なう処理を説明するための第１のフローチャートである。

【図１９】　２つのメモリカード間でコンテンツデータおよびキーデータ等の移動または複製を行なう処理を説明するための第２のフローチャートである。

【図２０】　実施の形態３のデータ配信システムの構成を説明するための概念図である。

【図２１】　実施の形態３のコンテンツデータ販売機２０００の構成を示す概略ブロック図である。

【図２２】　図２０および図２１で説明したデータ配信システムにおける配信モードを説明するための第１のフローチャートである。

【図２３】　図２０および図２１で説明したデータ配信システムにおける配信モードを説明するための第２のフローチャートである。

【図２４】　実施の形態３の変形例のコンテンツデータ販売機２００１の構成を示す概念図である。

【図２５】　実施の形態３の変形例のデータ配信システムにおける配信モードを説明するための第１のフローチャートである。

【図２６】　実施の形態３の変形例のデータ配信システムにおける配信モードを説明するための第２のフローチャートである。

【図２７】　実施の形態４のコンテンツデータ販売機３０００の構成を説明するための概略ブロック図である。

【図２８】　図２７で説明したデータ配信システムにおける配信モードを説明するための第１のフローチャートである。

【図２９】　図２７で説明したデータ配信システムにおける配信モードを説

明するための第２のフローチャートである。

【図３０】　実施の形態４の変形例のデータ配信システムにおける配信モードを説明するための第１のフローチャートである。

【図３１】　実施の形態４の変形例のデータ配信システムにおける配信モードを説明するための第２のフローチャートである。

【図３２】　実施の形態５における携帯電話機１０５の構成を説明するための概略ブロック図である。

【図３３】　実施の形態５のメモリカード１４０に対応した配信サーバ１２の構成を示す概略ブロック図である。

【図３４】　本発明の実施の形態５のメモリカード１４０の構成を説明するための概略ブロック図である。

【図３５】　メモリカード１４０を用いた配信モードを説明するための第１のフローチャートである。

【図３６】　メモリカード１４０を用いた配信モードを説明するための第２のフローチャートである。

【図３７】　メモリカード１４０に保持された暗号化コンテンツデータから、音楽として外部に出力するための再生処理を説明する第１のフローチャートである。

【図３８】　メモリカード１４０に保持された暗号化コンテンツデータから、音楽として外部に出力するための再生処理を説明する第２のフローチャートである。

【図３９】　２つのメモリカード間において、コンテンツデータおよびキーデータ等の移動または複製を行なう処理を説明するための第１のフローチャートである。

【図４０】　２つのメモリカード間において、コンテンツデータおよびキーデータ等の移動または複製を行なう処理を説明するための第２のフローチャートである。

【図４１】　本発明の実施の形態６のコンテンツデータ販売機３０１０の構成を示す概略ブロック図である。

【図４２】　コンテンツデータ販売機３０１０を用いたデータ配信システムにおける配信モードを説明するための第１のフローチャートである。

【図４３】　コンテンツデータ販売機３０１０を用いたデータ配信システムにおける配信モードを説明するための第２のフローチャートである。

【図４４】　実施の形態７における携帯電話機１０７の構成を説明するための概略ブロック図である。

【図４５】　実施の形態７の携帯電話機１０７に対応した配信サーバ１３の構成を示す概略ブロック図である。

【図４６】　配信サーバ１２と携帯電話機１０７を用いた配信モードを説明するための第１のフローチャートである。

【図４７】　配信サーバ１２と携帯電話機１０７を用いた配信モードを説明するための第２のフローチャートである。

【図４８】　メモリカード１４０に保持された暗号化コンテンツデータから、音楽として外部に出力するための再生処理を説明する第１のフローチャートである。

【図４９】　メモリカード１４０に保持された暗号化コンテンツデータから、音楽として外部に出力するための再生処理を説明する第２のフローチャートである。

【図５０】　実施の形態７において、２つのメモリカード間において、コンテンツデータおよびキーデータ等の移動または複製を行なう処理を説明するための第１のフローチャートである。

【図５１】　実施の形態７において、２つのメモリカード間において、コンテンツデータおよびキーデータ等の移動または複製を行なう処理を説明するための第２のフローチャートである。

【図５２】　本発明の実施の形態８のコンテンツデータ販売機３０２０の構成を示す概略ブロック図である。

【図５３】　コンテンツデータ販売機３０２０を用いたデータ配信システムにおける配信モードを説明するための第１のフローチャートである。

【図５４】　コンテンツデータ販売機３０２０を用いたデータ配信システム

における配信モードを説明するための第２のフローチャートである。

【図５５】　メモリカード１４０の端子１２０２部分の構成を説明する概略ブロック図である。

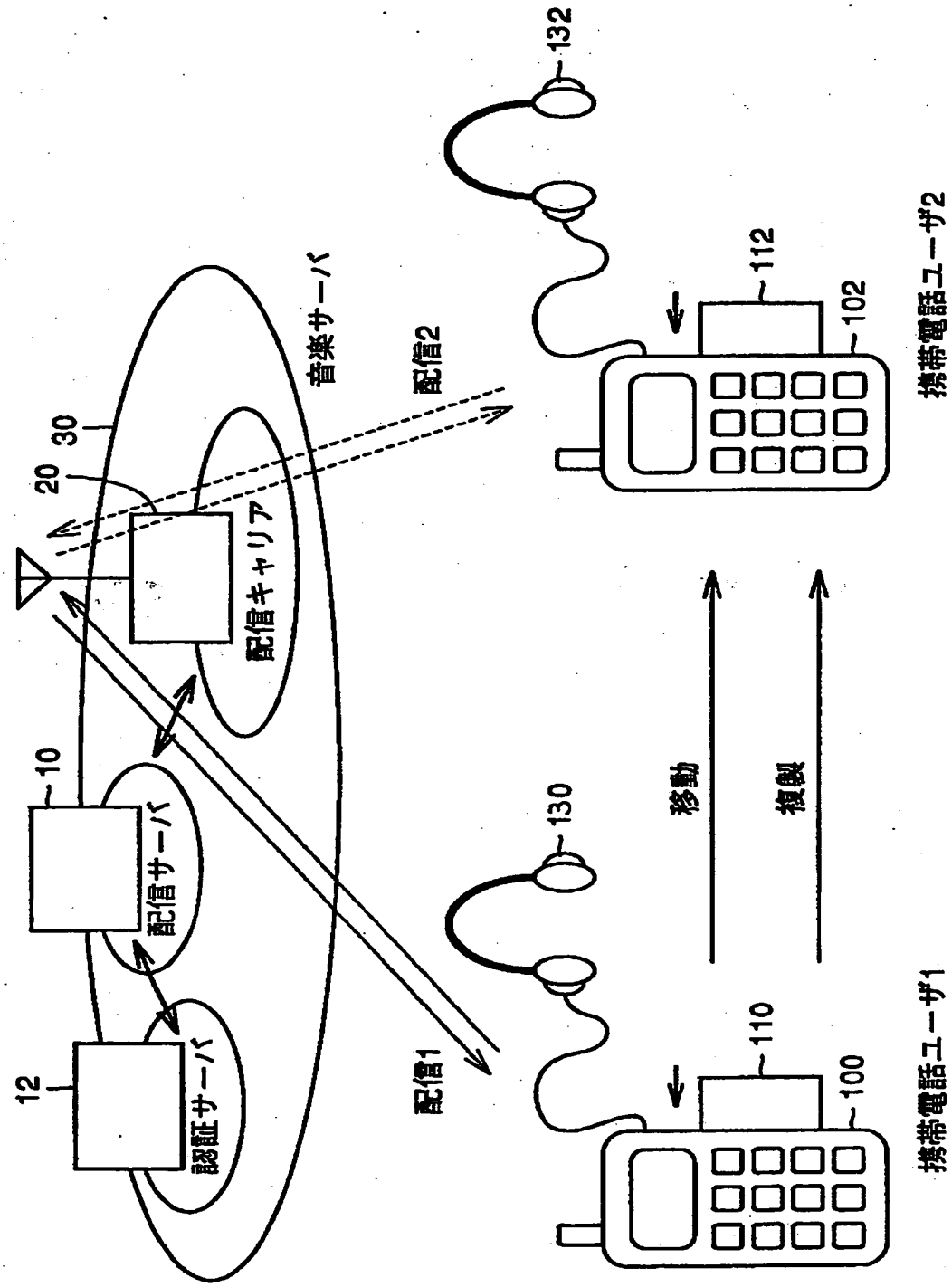
【図５６】　メモリカード１４０の端子１２０２部分の構成の変形例を説明するための概略ブロック図である。

【符号の説明】

１０，１１，１２，１３　配信サーバ、２０　配信キャリア、３０，３１　音楽サーバ、１００，１０１，１０２，１０３，１０５，１０６，１０７　携帯電話機、１１０，１１２，１２０，１２２，１４０，１４２　メモリカード、１３０，１３２　ヘッドホン、１１０２　アンテナ、１１０４　送受信機、１１０６　コントローラ、１１０８　タッチキー部、１１１０　ディスプレイ、１１１２　音声再生部、１２００　メモリインタフェース、１４０４　復号処理部、１４０６　暗号化処理部、１４０８，１４０９　切替スイッチ、１４１０　復号処理部、１４１２　メモリ、１４１４　暗号化処理部、１４１６　復号処理部、１４２０　コントローラ、１４３０　暗号化処理部、１４３２　セッションキー発生部、１４３４，１４３５　切替スイッチ、１５０２　セッションキー発生部、１５０４　暗号化処理部、１５０６　復号処理部、１５０８　音楽再生部、１５１０　混合部、１５１２　デジタルアナログ変換器、１５２５　[ＫＰｐ、Ｃｒｔｆ]ＫＰｍａｓｔｅｒ保持部、２０００，３０００，３０１０　コンテンツデータ販売機。

【書類名】　　図面

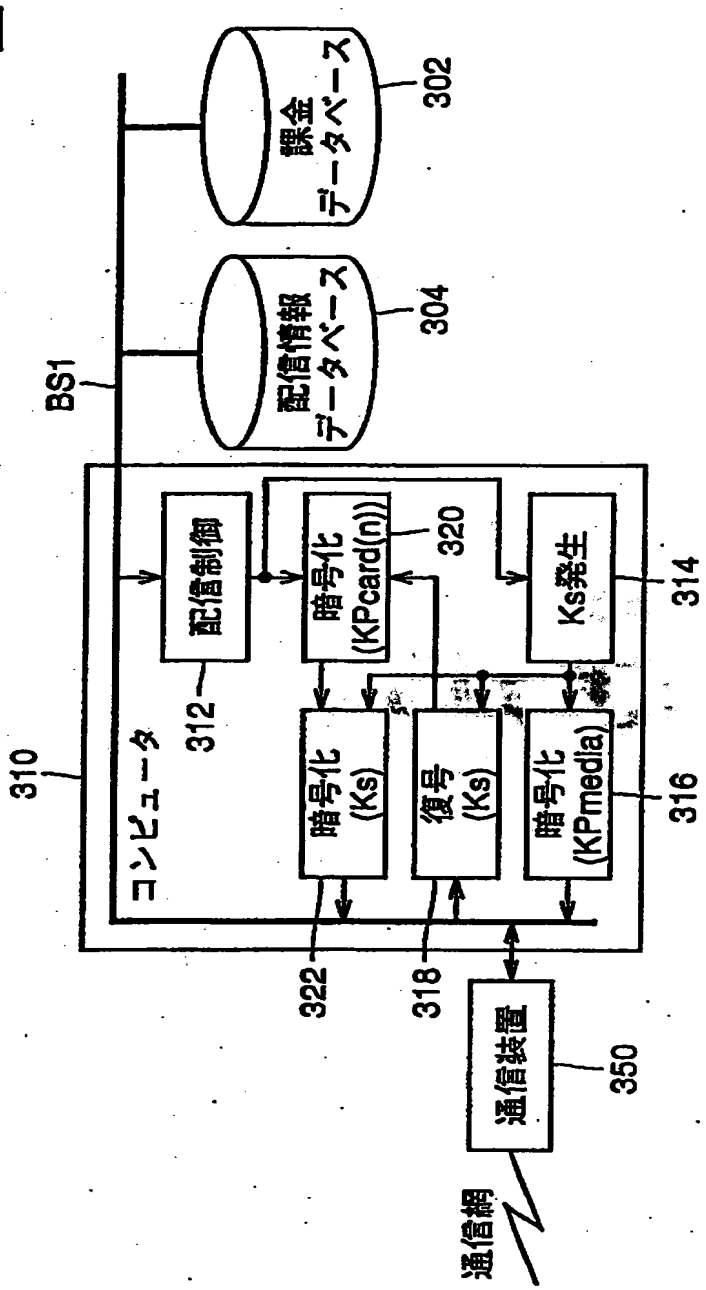
【図１】


132
112
102
携帯電話ユーザ2
音楽サーバ
配信2
30
20
配信キャリア
10
配信サーバ
12
認証サーバ
配信1
130
移動
複製
110
100
携帯電話ユーザ1

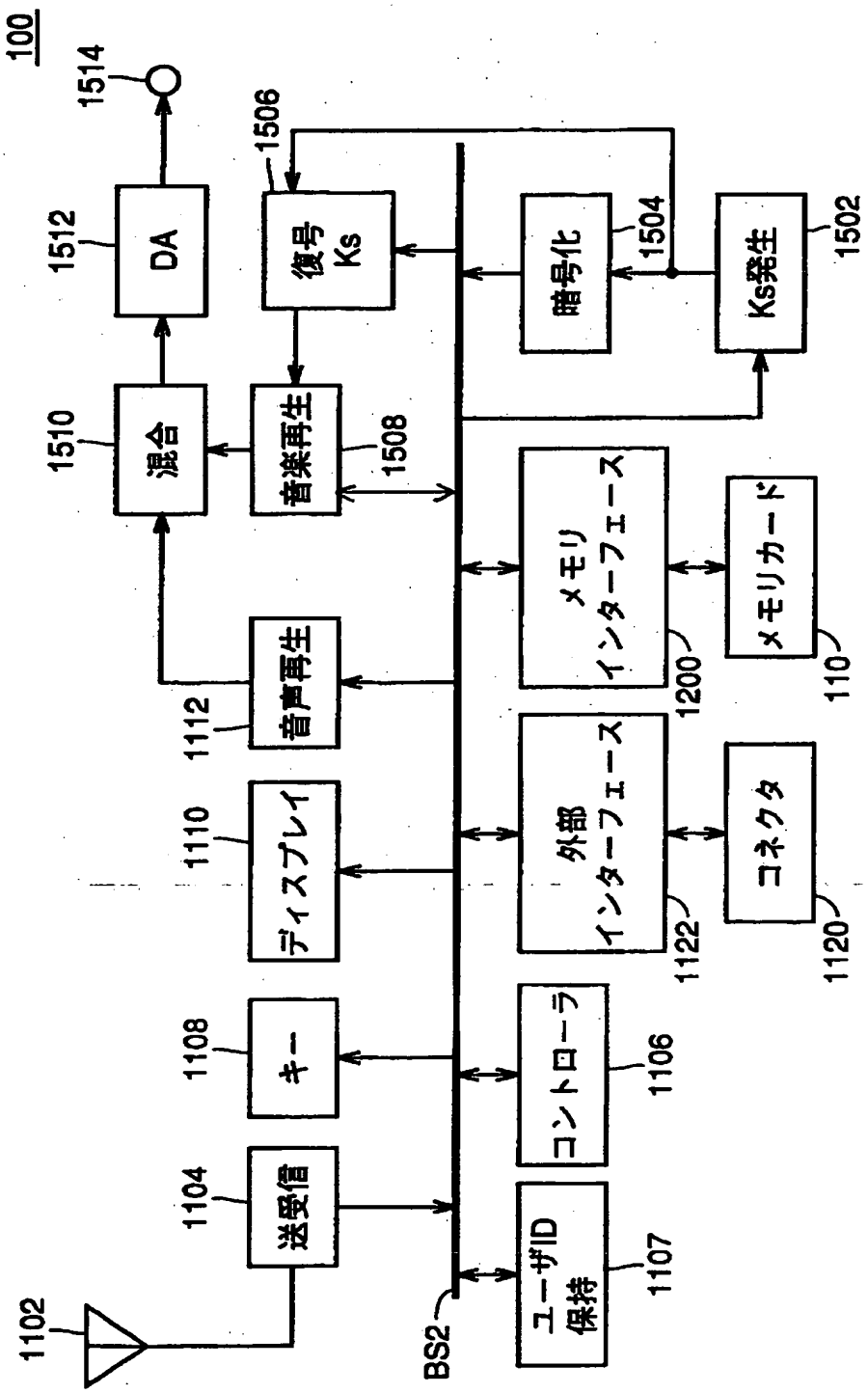
【図２】

	記号	属性	特性	
メモリカード内管理の鍵	Kmedia(n)	秘密復号鍵	媒体固有	メモリカードの種類ごとに固有な情報を有する
	Kcard(n)	秘密復号鍵		メモリカード毎に異なる
	KPcard(n)	公開暗号化鍵		Kcard(n)と対を成す。 KPcard(n)により暗号化されたデータは、Kcard(n)で復号可能
メモリカード外管理の鍵	KPmedia(n)	公開暗号化鍵	媒体固有	Kmediaと対を成す。 KPmediaにより暗号化されたデータは、Kmediaで復号可能。
	Ks	共通鍵	セッション固有	通信毎（例：アクセス毎）に発生。 配信サーバ、携帯電話機にて管理
配信データ	Kc	共通鍵	ライセンスキー	暗号化コンテンツデータの復号鍵
	License-ID	再生に関する情報		例：曲目の特定情報 再生回数の制限情報
	User-ID	受信者を識別する情報		例：電話番号
	Dc	コンテンツデータ		例：音楽
	[Dc]Kc	暗号化コンテンツデータ		共通鍵Kcにより暗号化されたコンテンツデータ

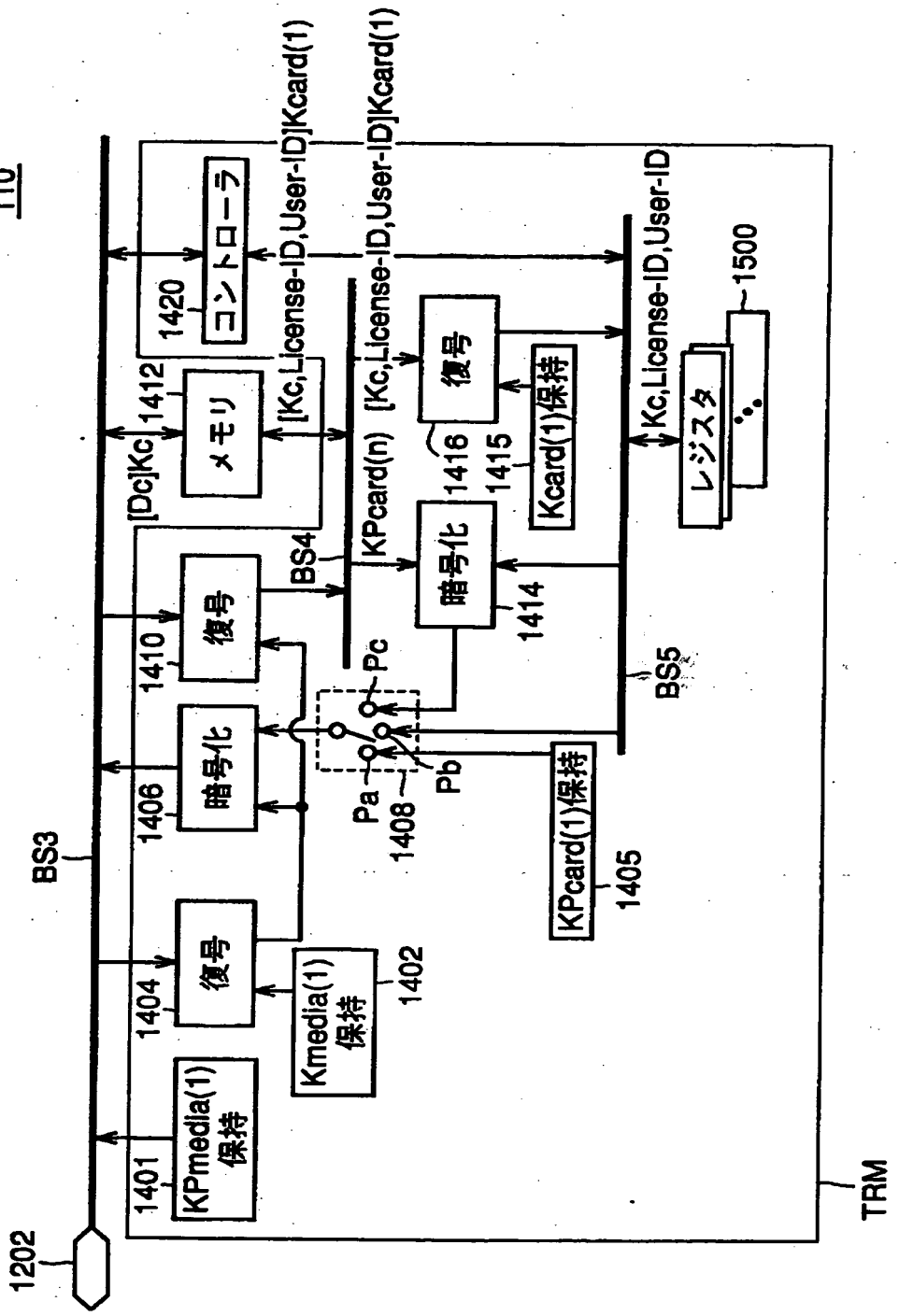
【図３】


10
課金データベース
302
配信情報データベース
304
BS1
配信制御
312
暗号化(KPcard(n))
320
Ks発生
314
コンピュータ
310
暗号化(Ks)
復号(Ks)
暗号化(KPmedia)
316
322
318
通信装置
350
通信網

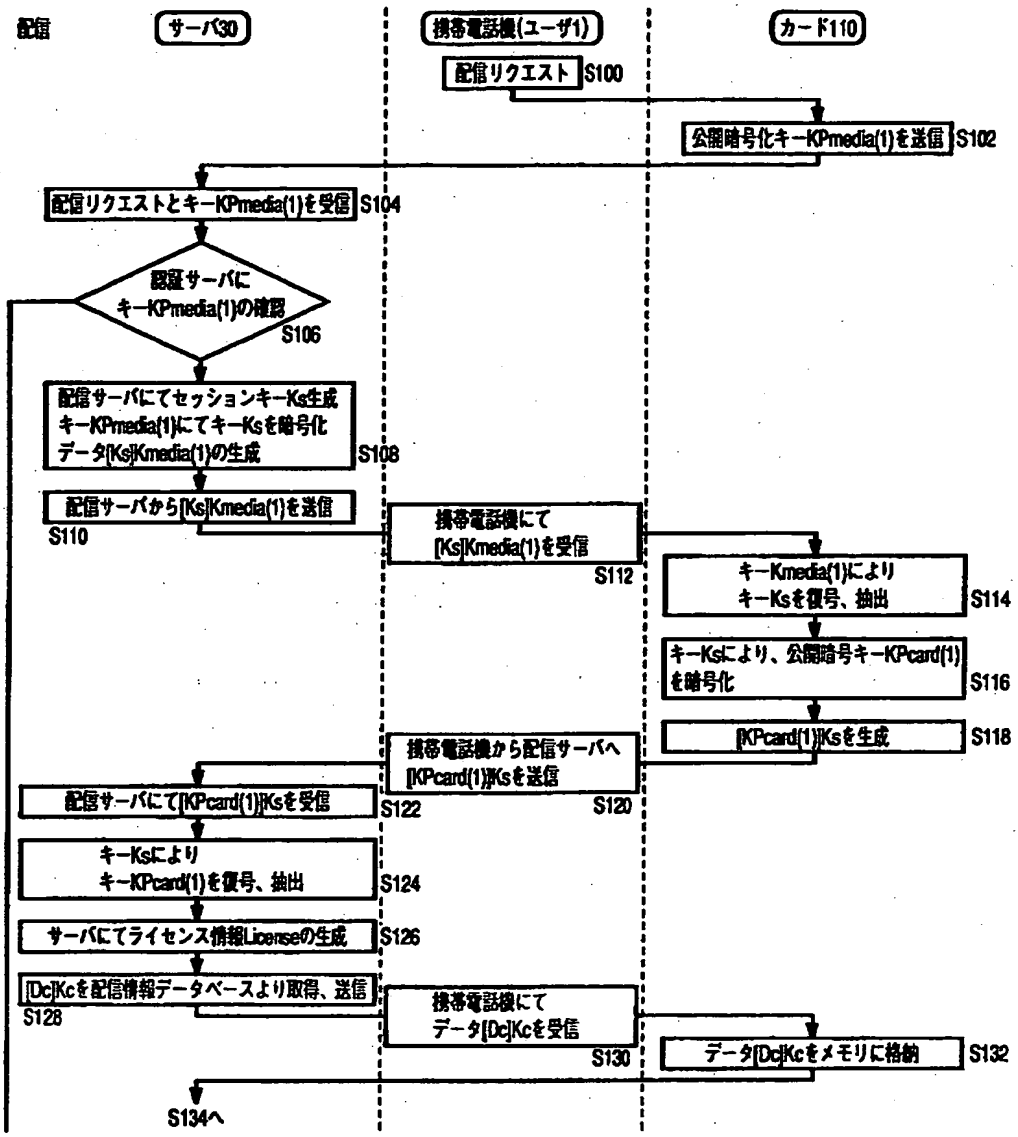
【図４】


100
1514
1506
1512
DA
復号
Ks
暗号化
1504
Ks発生
1502
1510
混合
音楽再生
1508
メモリ
インターフェース
メモリカード
1200
110
1112
音声再生
1110
ディスプレイ
外部
インターフェース
コネクタ
1122
1120
1108
キー
コントローラ
1106
1104
送受信
ユーザID
保持
1107
1102
BS2

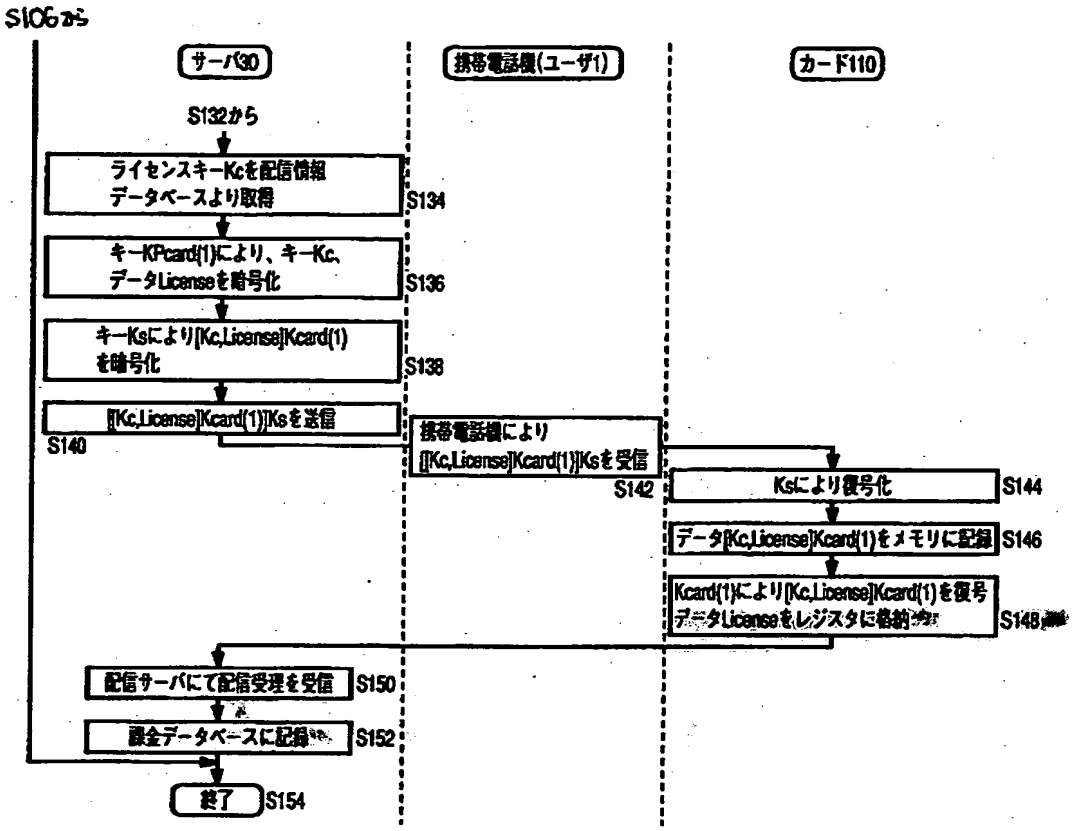
【図５】


110
コントローラ
1420
メモリ
1412
[Dc]Kc
[Kc,License-ID,User-ID]Kcard(1)
[Kc,License-ID,User-ID]Kcard(1)
Kc,License-ID,User-ID
1500
レジスタ
復号
1416
Kcard(1)保持
1415
暗号化
1414
KPcard(n)
BS4
BS5
Pc
Pa
Pb
1408
KPcard(1)保持
1405
復号
1410
暗号化
1406
復号
1404
Kmedia(1)保持
1402
KPmedia(1)保持
1401
BS3
1202
TRM

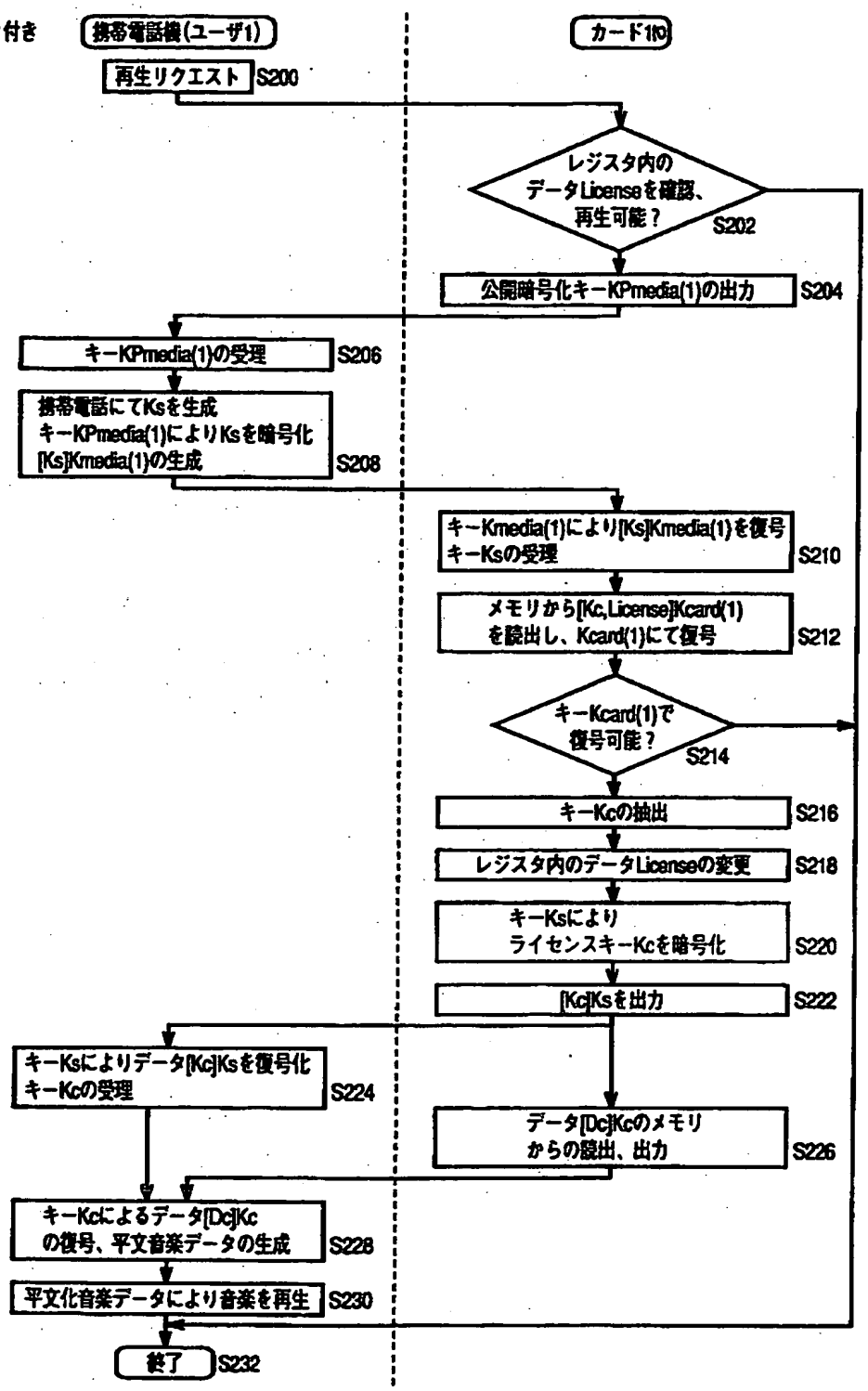
【図６】


配信
サーバ30
携帯電話機(ユーザ1)
カード110
配信リクエスト S100
公開暗号化キーKPmedia(1)を送信 S102
配信リクエストとキーKPmedia(1)を受信 S104
認証サーバにキーKPmedia(1)の確認 S106
配信サーバにてセッションキーKs生成 キーKPmedia(1)にてキーKsを暗号化 データ[Ks]Kmedia(1)の生成 S108
配信サーバから[Ks]Kmedia(1)を送信 S110
携帯電話機にて[Ks]Kmedia(1)を受信 S112
キーKmedia(1)によりキーKsを復号、抽出 S114
キーKsにより、公開暗号キーKPcard(1)を暗号化 S116
[KPcard(1)]Ksを生成 S118
携帯電話機から配信サーバへ[KPcard(1)]Ksを送信 S120
配信サーバにて[KPcard(1)]Ksを受信 S122
キーKsによりキーKPcard(1)を復号、抽出 S124
サーバにてライセンス情報Licenseの生成 S126
[Dc]Kcを配信情報データベースより取得、送信 S128
携帯電話機にてデータ[Dc]Kcを受信 S130
データ[Dc]Kcをメモリに格納 S132
S134へ

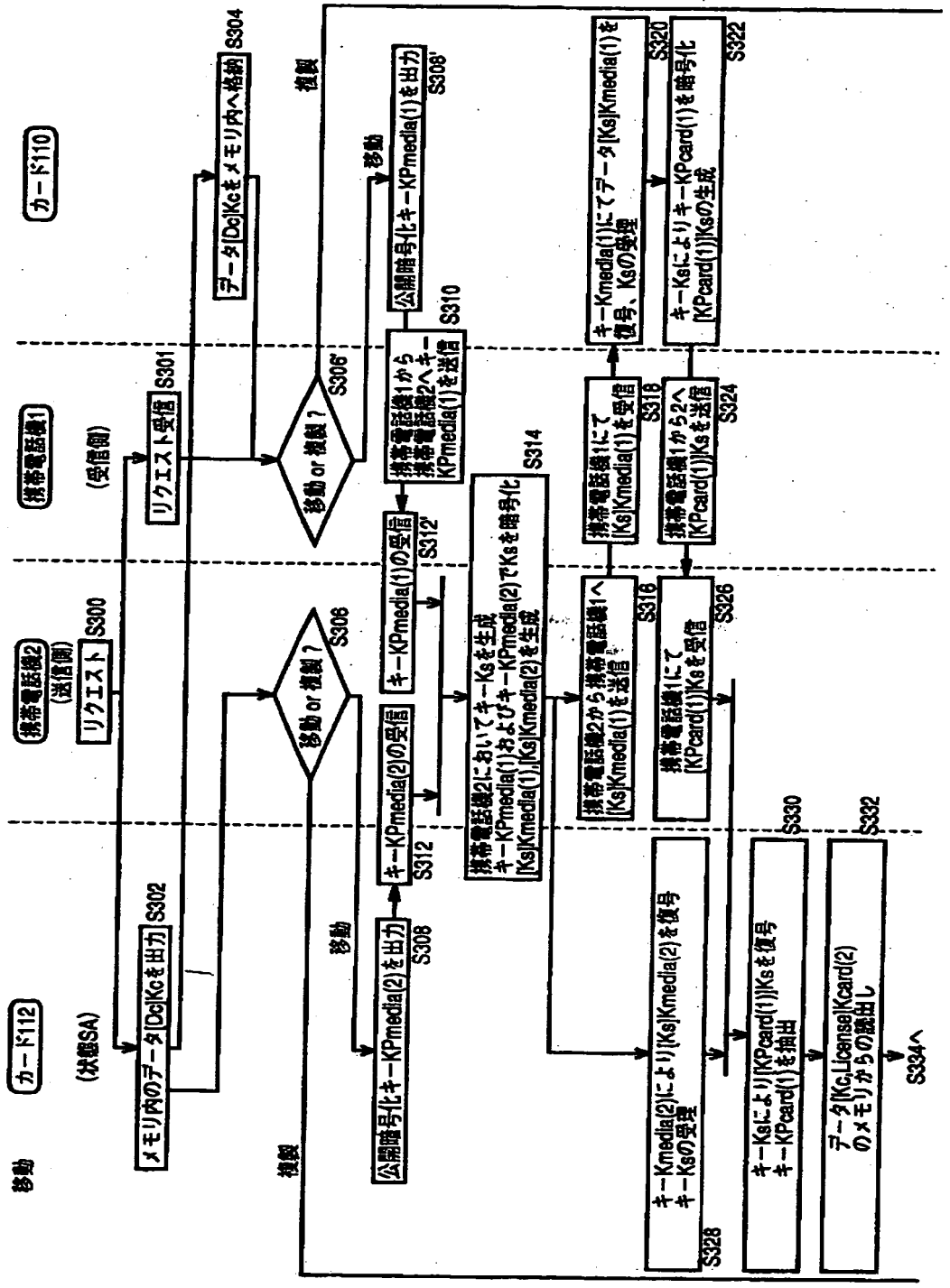
【図７】


S106から
サーバ30
携帯電話機(ユーザ1)
カード110
S132から
ライセンスキーKcを配信情報データベースより取得
S134
キーKPcard(1)により、キーKc、データLicenseを暗号化
S136
キーKsにより[Kc,License]Kcard(1)を暗号化
S138
[[Kc,License]Kcard(1)]Ksを送信
S140
携帯電話機により[[Kc,License]Kcard(1)]Ksを受信
S142
Ksにより復号化
S144
データ[Kc,License]Kcard(1)をメモリに記録
S146
Kcard(1)により[Kc,License]Kcard(1)を復号データLicenseをレジスタに格納
S148
配信サーバにて配信受理を受信
S150
課金データベースに記録
S152
終了
S154

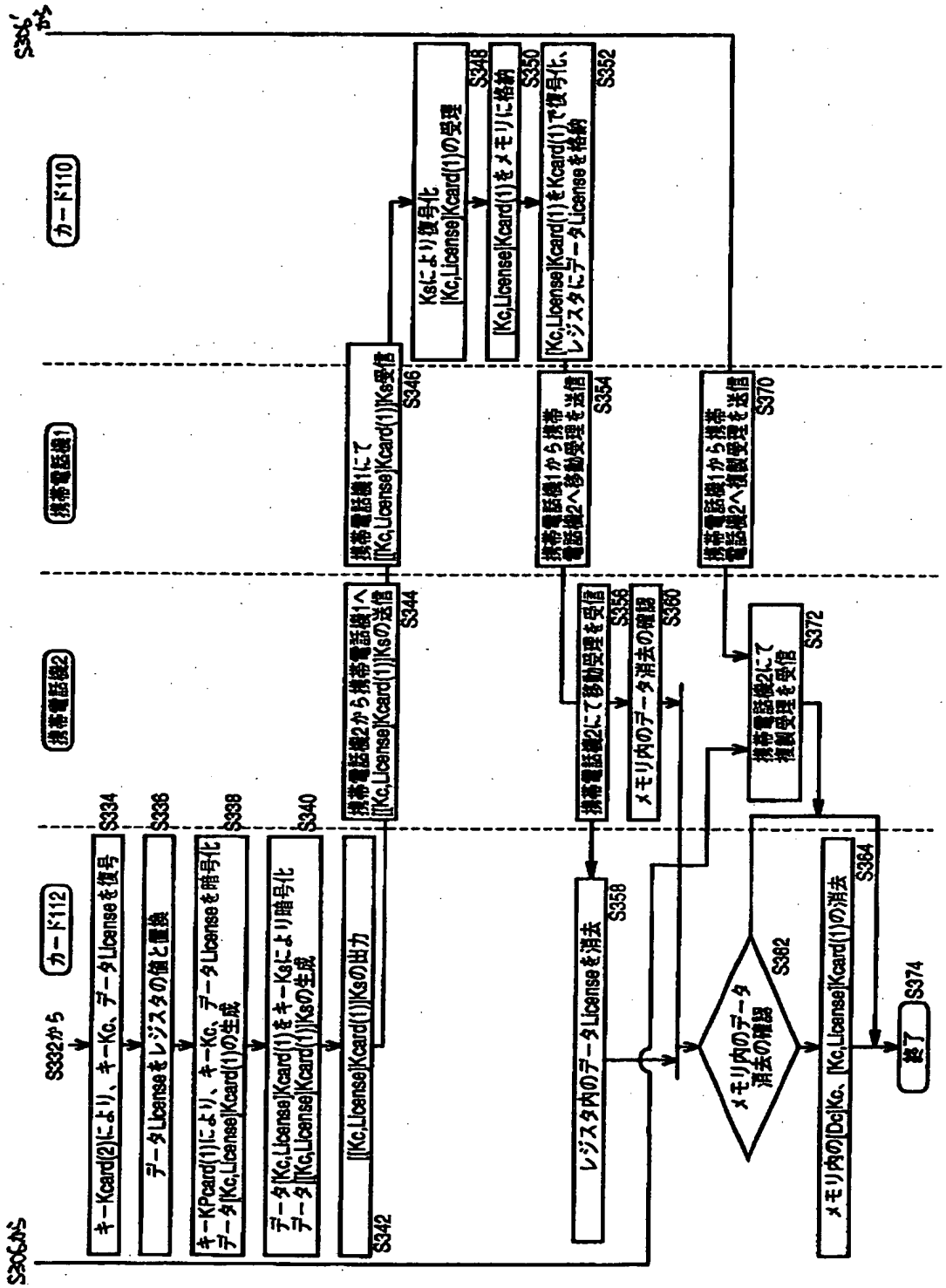
【図８】


レジスタ付き再生
携帯電話機(ユーザ1)
カード1
再生リクエスト S200
レジスタ内のデータLicenseを確認、再生可能？ S202
公開暗号化キーKPmedia(1)の出力 S204
キーKPmedia(1)の受理 S206
携帯電話にてKsを生成 キーKPmedia(1)によりKsを暗号化 [Ks]Kmedia(1)の生成 S208
キーKmedia(1)により[Ks]Kmedia(1)を復号 キーKsの受理 S210
メモリから[Kc,License]Kcard(1)を読出し、Kcard(1)にて復号 S212
キーKcard(1)で復号可能？ S214
キーKcの抽出 S216
レジスタ内のデータLicenseの変更 S218
キーKsによりライセンスキーKcを暗号化 S220
[Kc]Ksを出力 S222
キーKsによりデータ[Kc]Ksを復号化 キーKcの受理 S224
データ[Dc]Kcのメモリからの読出、出力 S226
キーKcによるデータ[Dc]Kcの復号、平文音楽データの生成 S228
平文化音楽データにより音楽を再生 S230
終了 S232

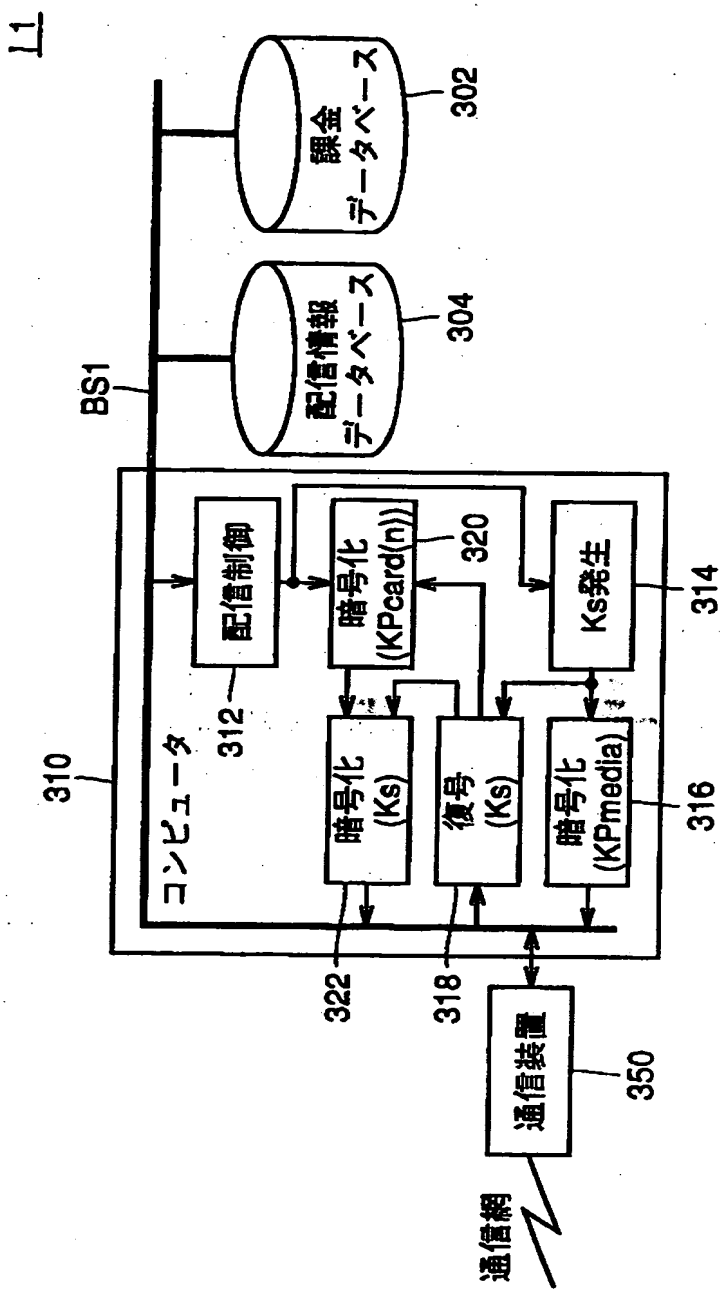
【図９】


移動
カード112
(状態SA)
メモリ内のデータ[Dc]Kcを出力 S302
公開暗号化キーKPmedia(2)を出力 S308
キーKPmedia(2)の受信 S312
携帯電話線2
(送信側)
リクエスト S300
移動 or 複製? S306
携帯電話線1
(受信側)
リクエスト受信 S301
データ[Dc]Kcをメモリ内へ格納 S304
移動 or 複製? S306'
公開暗号化キーKPmedia(1)を出力 S308'
キーKPmedia(1)の受信 S312'
携帯電話線2において
キーKPmedia(1)およびキーKPmedia(2)でKsを暗号化
[Ks]Kmedia(1),[Ks]Kmedia(2)を生成 S314
携帯電話線2から携帯電話線1へ
[Ks]Kmedia(1)を送信 S316
携帯電話線1にて
[Ks]Kmedia(1)を受信 S318
携帯電話線1から2へ
[KPcard(1)]Ksを送信 S324
キーKmedia(1)にてデータ[Ks]Kmedia(1)を
復号、Ksの受理 S320
キーKsにより キーKPcard(1)を暗号化
[KPcard(1)]Ksの生成 S322
携帯電話線1にて
[KPcard(1)]Ksを受信 S326
キーKmedia(2)により[Ks]Kmedia(2)を復号
キーKsの受理 S328
キーKsにより[KPcard(1)]Ksを復号
キーKPcard(1)を抽出 S330
データ[Kc,License]Kcard(2)
のメモリからの読出し S332
S334へ
複製
移動
複製

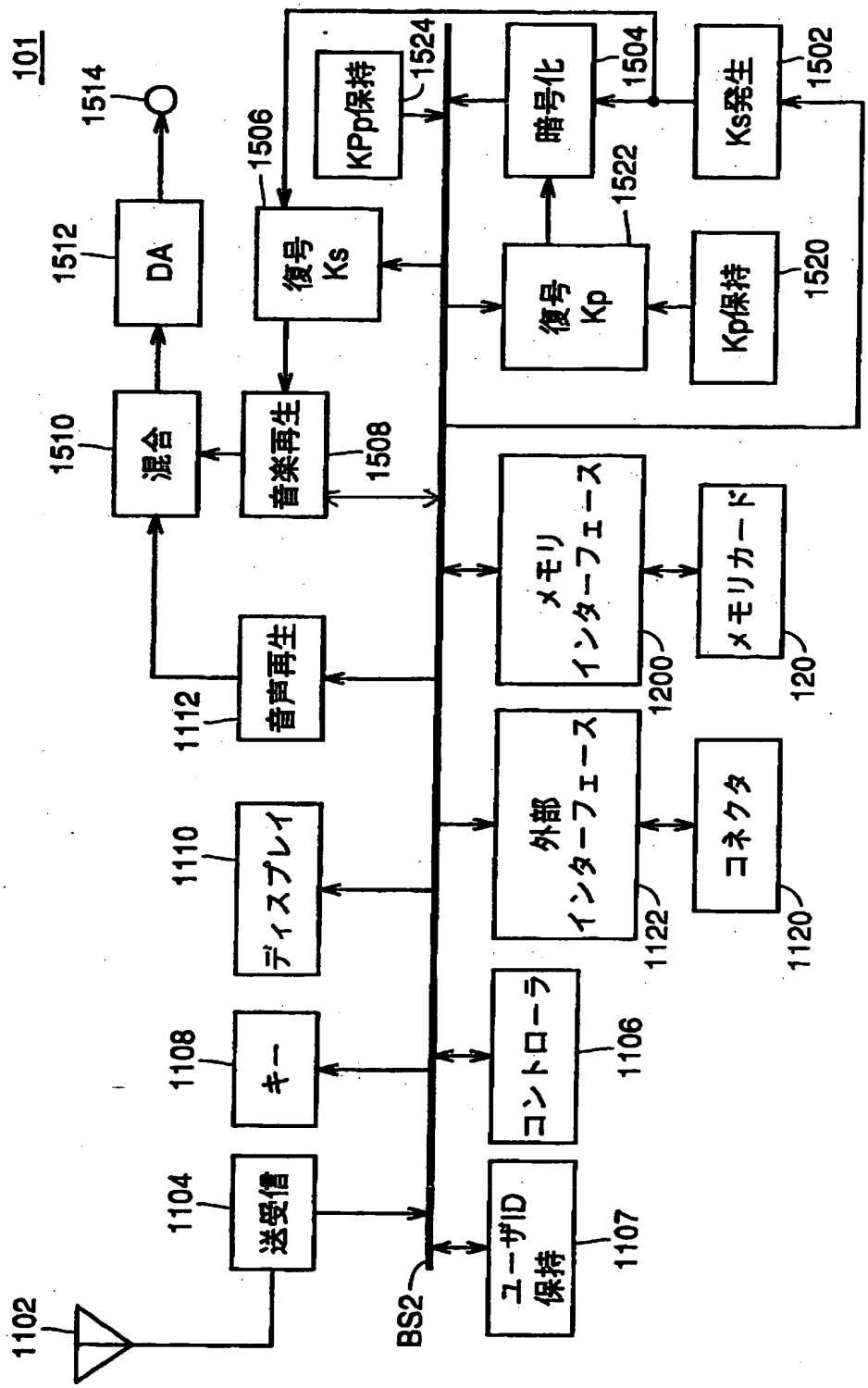
【図１０】


S306から
カード110
携帯電話機1
携帯電話機2
カード112
S332から
S334
キーKcard(2)により、キーKc、データLicenseを復号
S336
データLicenseをレジスタの値と置換
S338
キーKPcard(1)により、キーKc、データLicenseを暗号化
データ[Kc,License]Kcard(1)の生成
S340
データ[Kc,License]Kcard(1)をキーKsにより暗号化
データ[[Kc,License]Kcard(1)]Ksの生成
S342
[[Kc,License]Kcard(1)]Ksの出力
S344
携帯電話機2から携帯電話機1へ
[[Kc,License]Kcard(1)]Ksの送信
S346
携帯電話機1にて
[[Kc,License]Kcard(1)]Ks受信
S348
Ksにより復号化
[Kc,License]Kcard(1)の受理
S350
[Kc,License]Kcard(1)をメモリに格納
S352
[Kc,License]Kcard(1)をKcard(1)で復号化、
レジスタにデータLicenseを格納
S354
携帯電話機1から携帯
電話機2へ移動受理を送信
S356
携帯電話機2にて移動受理を受信
S358
レジスタ内のデータLicenseを消去
S360
メモリ内のデータ消去の確認
S362
メモリ内のデータ
消去の確認
S364
メモリ内の[Dc]Kc、[Kc,License]Kcard(1)の消去
S370
携帯電話機1から携帯
電話機2へ複製受理を送信
S372
携帯電話機2にて
複製受理を受信
S374
終了
S306から

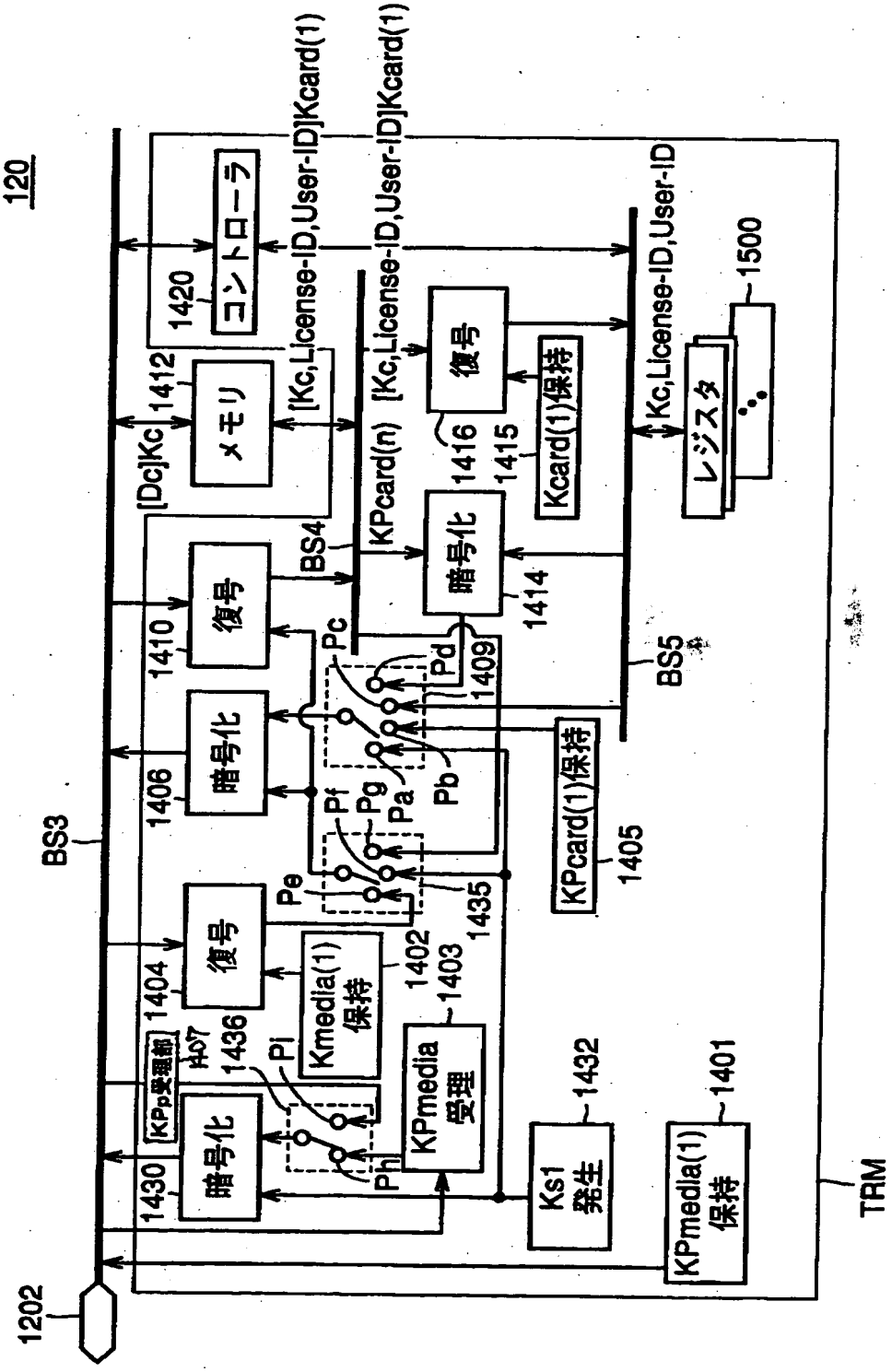
【図１１】


11
課金データベース
302
配信情報データベース
304
BS1
配信制御
312
暗号化(KPcard(n))
320
Ks発生
314
コンピュータ
310
暗号化(Ks)
復号(Ks)
暗号化(KPmedia)
316
322
318
通信装置
350
通信網

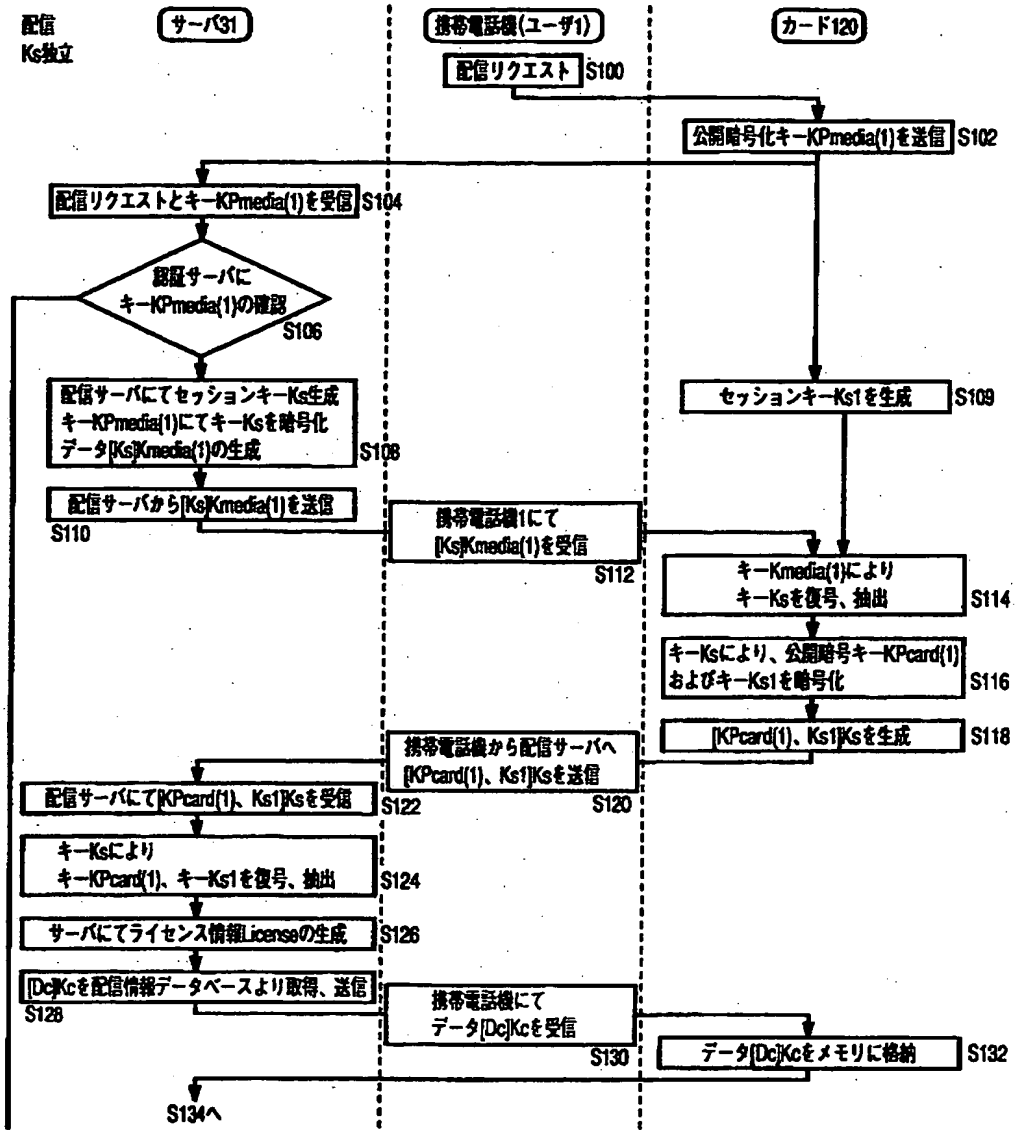
【図１２】


101
1514
DA
1512
混合
1510
音声再生
1112
ディスプレイ
1110
キー
1108
送受信
1104
1102
BS2
ユーザID保持
1107
コントローラ
1106
外部インターフェース
1122
コネクタ
1120
メモリインターフェース
1200
メモリカード
120
音楽再生
1508
復号Ks
1506
KPp保持
1524
復号Kp
1522
Kp保持
1520
暗号化
1504
Ks発生
1502

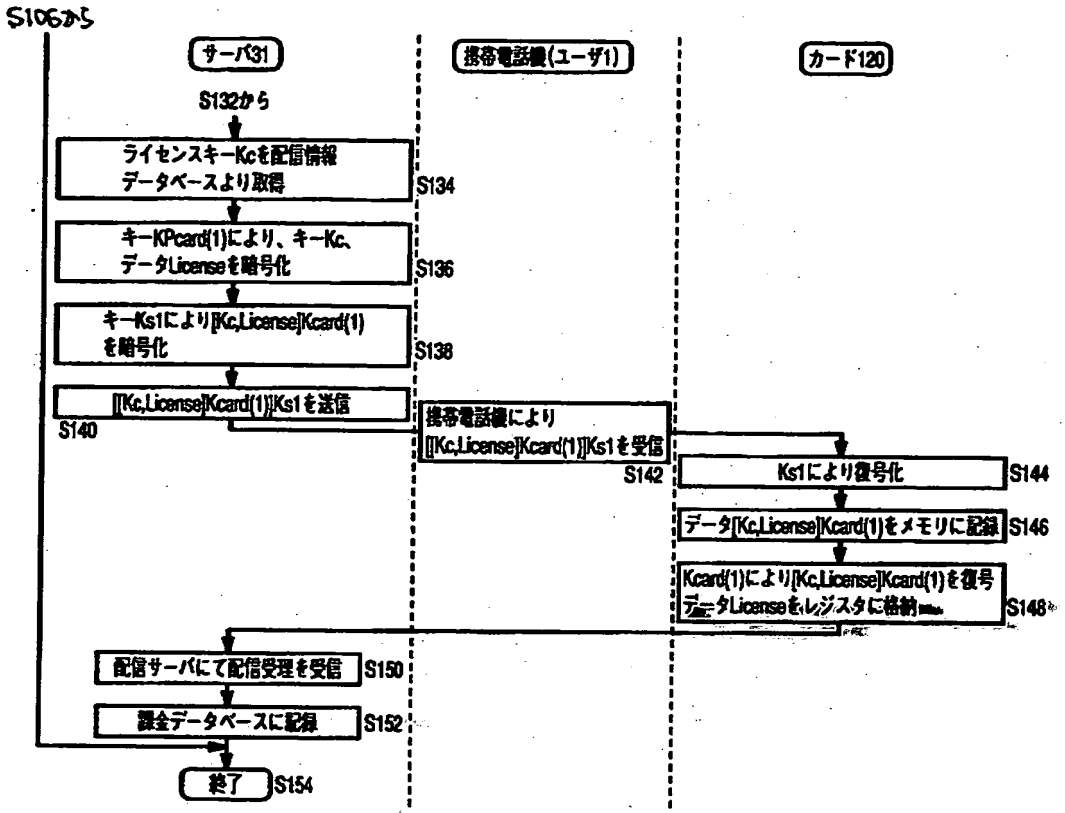
【図１３】


120
コントローラ
1420
メモリ
1412
[Dc]Kc
[Kc,License-ID,User-ID]Kcard(1)
[Kc,License-ID,User-ID]Kcard(1)
[Kc,License-ID,User-ID
1500
レジスタ
復号
1416
Kcard(1)保持
1415
暗号化
1414
KPcard(n)
BS4
BS5
復号
1410
暗号化
1406
復号
1404
KPp受理部
407
1436
暗号化
1430
Kmedia(1)保持
1402
KPmedia受理
1403
Ks1発生
1432
KPmedia(1)保持
1401
KPcard(1)保持
1405
1409
1435
BS3
Pa
Pb
Pc
Pd
Pe
Pf
Pg
Ph
Pi
1202
TRM

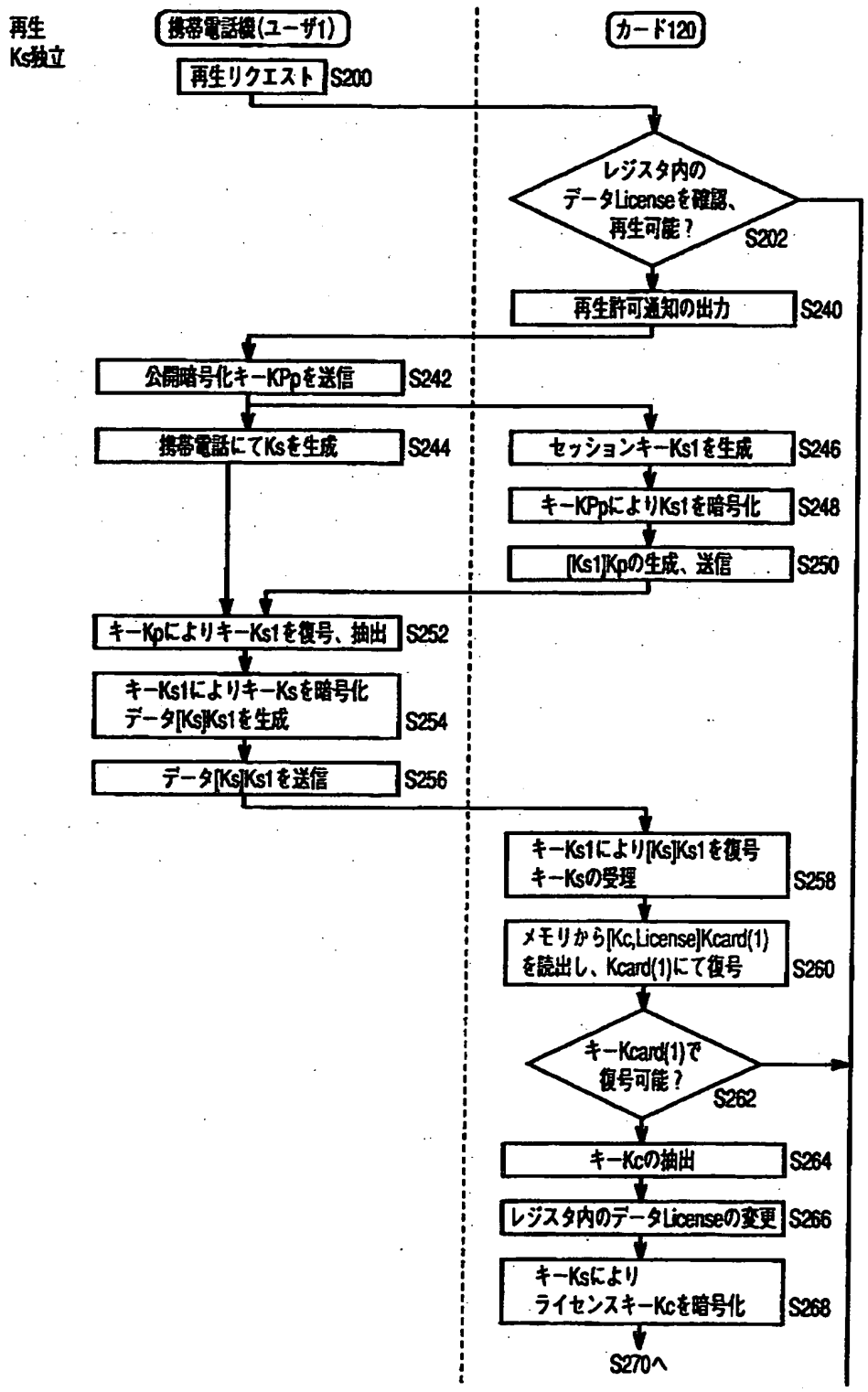
【図１４】


配信
Ks独立
サーバ31
携帯電話機(ユーザ1)
カード120
配信リクエスト S100
公開暗号化キーKPmedia(1)を送信 S102
配信リクエストとキーKPmedia(1)を受信 S104
認証サーバに
キーKPmedia(1)の確認
S106
配信サーバにてセッションキーKs生成
キーKPmedia(1)にてキーKsを暗号化
データ[Ks]Kmedia(1)の生成 S108
セッションキーKs1を生成 S109
配信サーバから[Ks]Kmedia(1)を送信
S110
携帯電話機1にて
[Ks]Kmedia(1)を受信
S112
キーKmedia(1)により
キーKsを復号、抽出 S114
キーKsにより、公開暗号キーKPcard(1)
およびキーKs1を暗号化 S116
[KPcard(1)、Ks1]Ksを生成 S118
携帯電話機から配信サーバへ
[KPcard(1)、Ks1]Ksを送信
S120
配信サーバにて[KPcard(1)、Ks1]Ksを受信
S122
キーKsにより
キーKPcard(1)、キーKs1を復号、抽出 S124
サーバにてライセンス情報Licenseの生成 S126
[Dc]Kcを配信情報データベースより取得、送信
S128
携帯電話機にて
データ[Dc]Kcを受信
S130
データ[Dc]Kcをメモリに格納 S132
S134へ

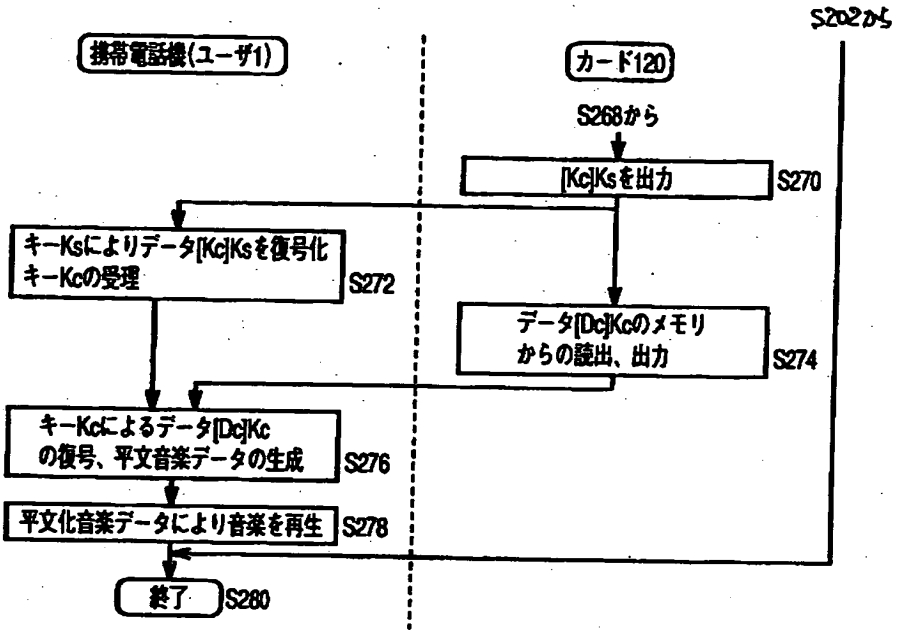
【図１５】


S106から
サーバ31
携帯電話機(ユーザ1)
カード120
S132から
ライセンスキーKcを配信情報データベースより取得
S134
キーKPcard(1)により、キーKc、データLicenseを暗号化
S136
キーKs1により[Kc,License]Kcard(1)を暗号化
S138
[[Kc,License]Kcard(1)]Ks1を送信
S140
携帯電話機により[[Kc,License]Kcard(1)]Ks1を受信
S142
Ks1により復号化
S144
データ[Kc,License]Kcard(1)をメモリに記録
S146
Kcard(1)により[Kc,License]Kcard(1)を復号データLicenseをレジスタに格納
S148
配信サーバにて配信受理を受信
S150
課金データベースに記録
S152
終了
S154

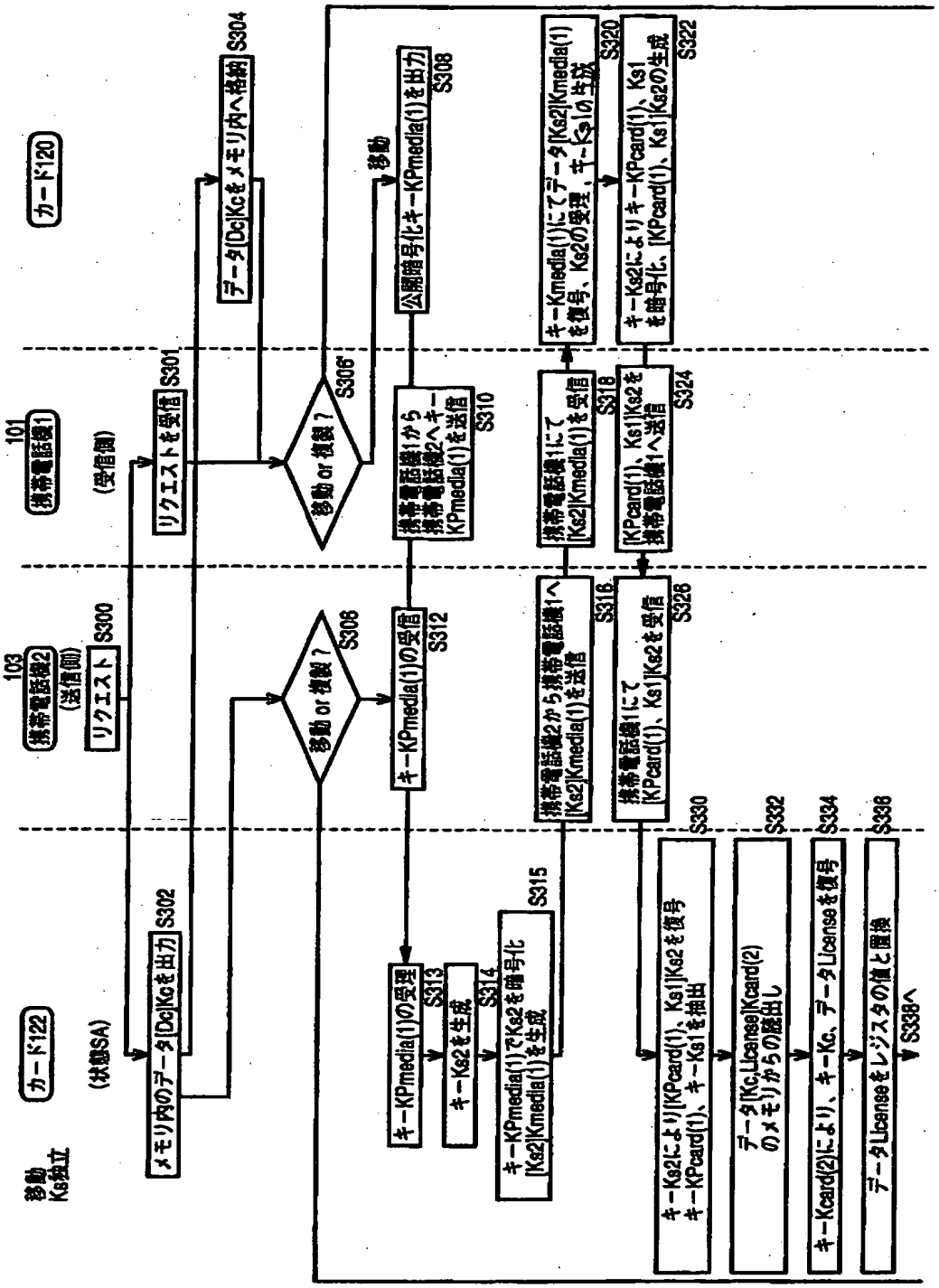
【図１６】


再生
Ks独立
携帯電話機(ユーザ1)
カード120
再生リクエスト S200
レジスタ内のデータLicenseを確認、再生可能？ S202
再生許可通知の出力 S240
公開暗号化キーKPpを送信 S242
携帯電話にてKsを生成 S244
セッションキーKs1を生成 S246
キーKPpによりKs1を暗号化 S248
[Ks1]Kpの生成、送信 S250
キーKpによりキーKs1を復号、抽出 S252
キーKs1によりキーKsを暗号化データ[Ks]Ks1を生成 S254
データ[Ks]Ks1を送信 S256
キーKs1により[Ks]Ks1を復号キーKsの受理 S258
メモリから[Kc,License]Kcard(1)を読出し、Kcard(1)にて復号 S260
キーKcard(1)で復号可能？ S262
キーKcの抽出 S264
レジスタ内のデータLicenseの変更 S266
キーKsによりライセンスキーKcを暗号化 S268
S270へ

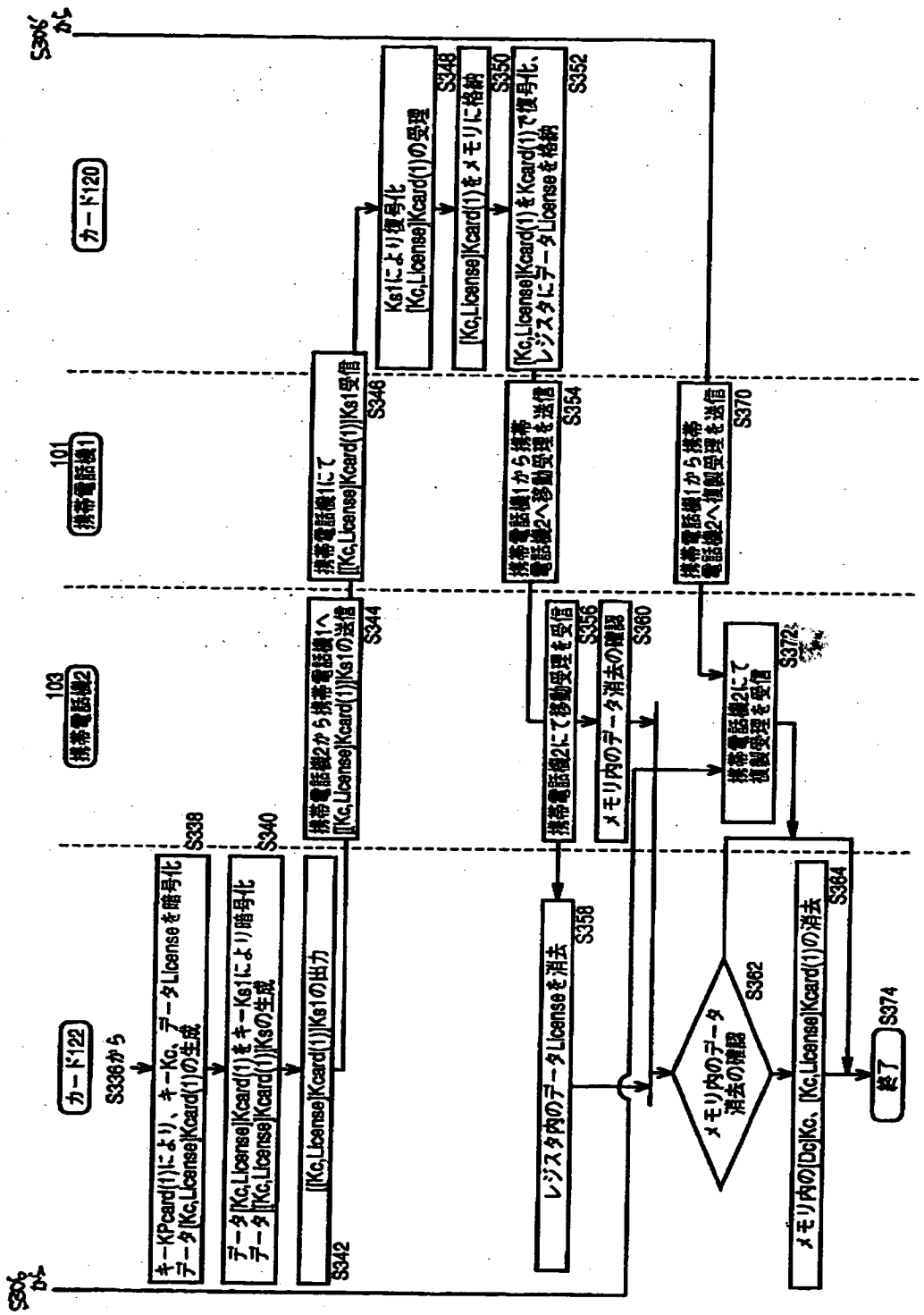
【図１７】


S202から
携帯電話機(ユーザ1)
カード120
S268から
[Kc]Ksを出力
S270
キーKsによりデータ[Kc]Ksを復号化
キーKcの受理
S272
データ[Dc]Kcのメモリ
からの読出、出力
S274
キーKcによるデータ[Dc]Kc
の復号、平文音楽データの生成
S276
平文化音楽データにより音楽を再生
S278
終了
S280

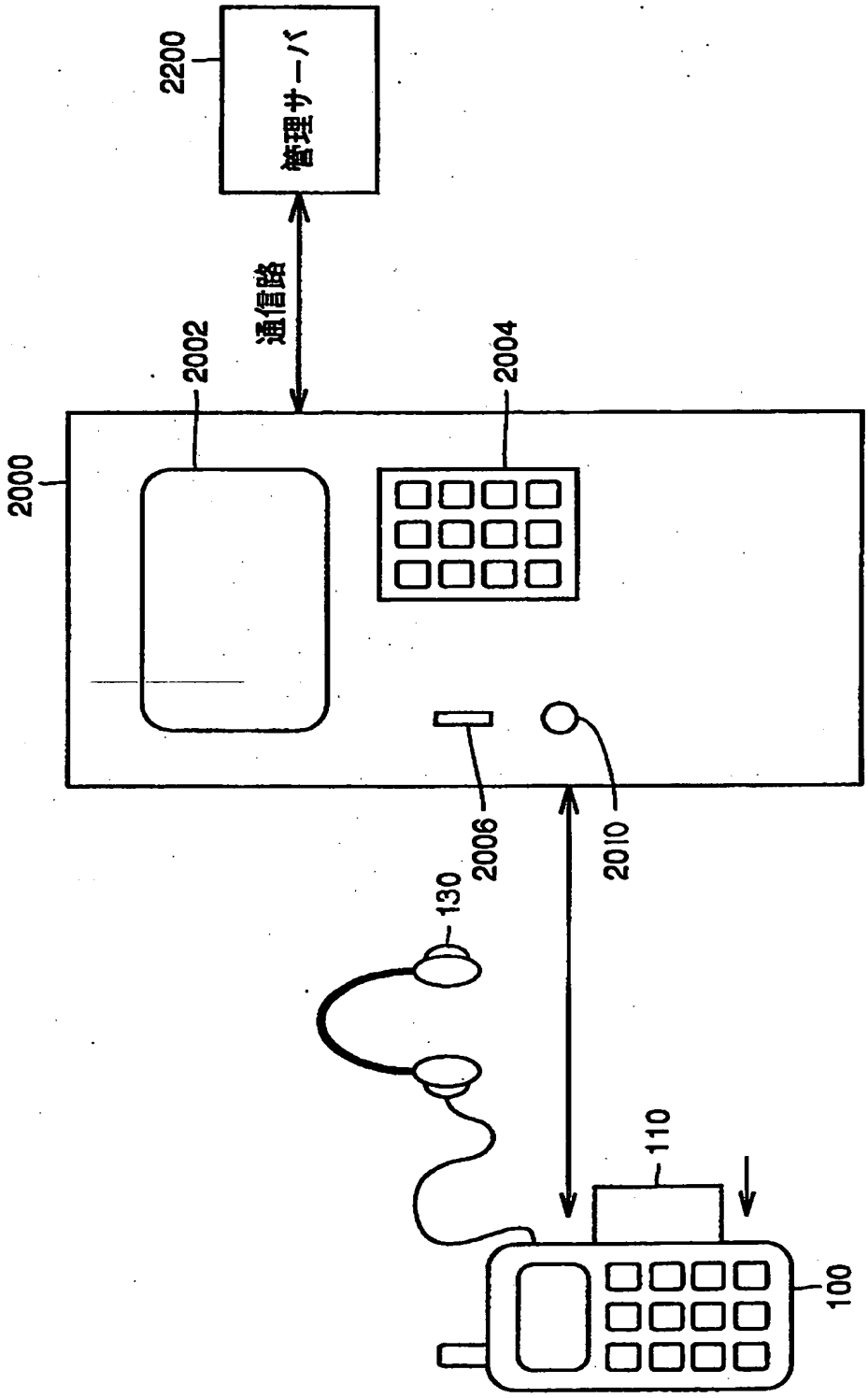
【図１８】


移動
Ks独立
カード122
(共通SA)
メモリ内のデータ[Dc]Kcを出力 S302
カード120
データ[Dc]Kcをメモリ内へ格納 S304
101
携帯電話機1
(受信側)
リクエストを受信 S301
移動 or 複製？ S306'
移動
公開暗号化キーKPmedia(1)を出力 S308
103
携帯電話機2
(送信側)
リクエスト S300
移動 or 複製？ S306
キーKPmedia(1)の受信 S312
携帯電話機1から携帯電話機2へキーKPmedia(1)を送信 S310
キーKPmedia(1)の受理 S313
キーKs2を生成 S314
キーKPmedia(1)でKs2を暗号化[Ks2]Kmedia(1)を生成 S315
携帯電話機2から携帯電話機1へ[Ks2]Kmedia(1)を送信 S316
携帯電話機1にて[Ks2]Kmedia(1)を受信 S318
キーKmedia(1)にてデータ[Ks2]Kmedia(1)を復号、Ks2の受理，キーKs1の生成 S320
キーKs2によりキーKPcard(1)、Ks1を暗号化、[KPcard(1)、Ks1]Ks2の生成 S322
[KPcard(1)、Ks1]Ks2を携帯電話機1へ送信 S324
携帯電話機1にて[KPcard(1)、Ks1]Ks2を受信 S326
携帯電話機1にて[KPcard(1)、Ks1]Ks2を受信 S328
キーKs2により[KPcard(1)、Ks1]Ks2を復号 キーKPcard(1)、キーKs1を抽出 S330
データ[Kc,License]Kcard(2)のメモリからの読出し S332
キーKcard(2)により、キーKc、データLicenseを復号 S334
データLicenseをレジスタの値と置換 S336
S338へ

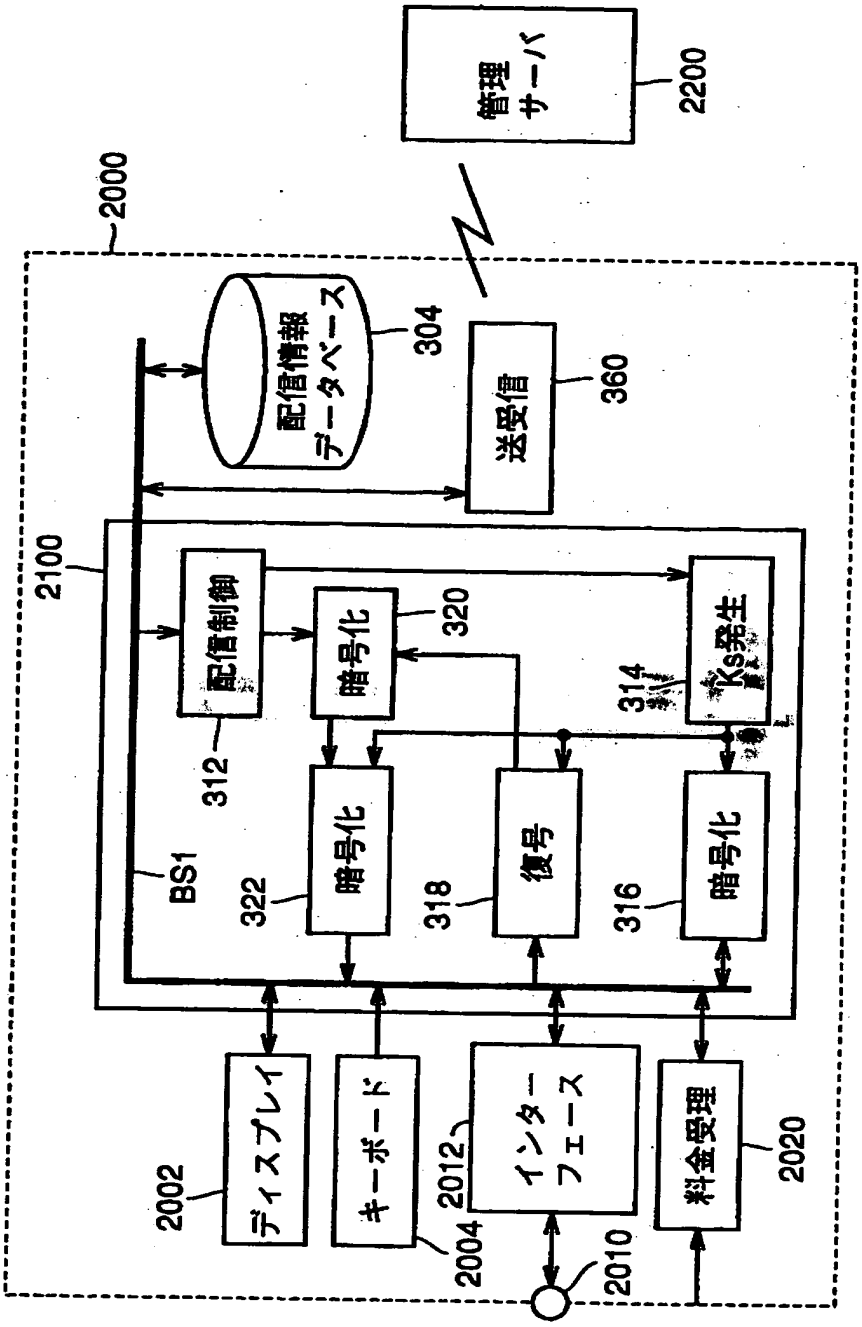
【図１９】


S306から
カード120
携帯電話機1
101
携帯電話機2
103
カード122
S336から
S338
S340
S342
S344
S346
S348
S350
S352
S354
S356
S358
S360
S362
S370
S372
S374
S384
S306へ
キーKPcard(1)により、キーKc、データLicenseを暗号化
データ{Kc,License}Kcard(1)の生成
データ{Kc,License}Kcard(1)をキーKs1により暗号化
データ{{Kc,License}Kcard(1)}Ksの生成
{{Kc,License}Kcard(1)}Ks1の出力
携帯電話機2から携帯電話機1へ{{Kc,License}Kcard(1)}Ks1の送信
携帯電話機1にて{{Kc,License}Kcard(1)}Ks1受信
Ks1により復号化{Kc,License}Kcard(1)の受理
{Kc,License}Kcard(1)をメモリに格納
{Kc,License}Kcard(1)をKcard(1)で復号化、レジスタにデータLicenseを格納
携帯電話機1から携帯電話機2へ移動受理を送信
携帯電話機2にて移動受理を受信
メモリ内のデータ消去の確認
レジスタ内のデータLicenseを消去
携帯電話機1から携帯電話機2へ複製受理を送信
携帯電話機2にて複製受理を受信
メモリ内のデータ消去の確認
メモリ内の{Dcj}Kc、{Kc,License}Kcard(1)の消去
終了

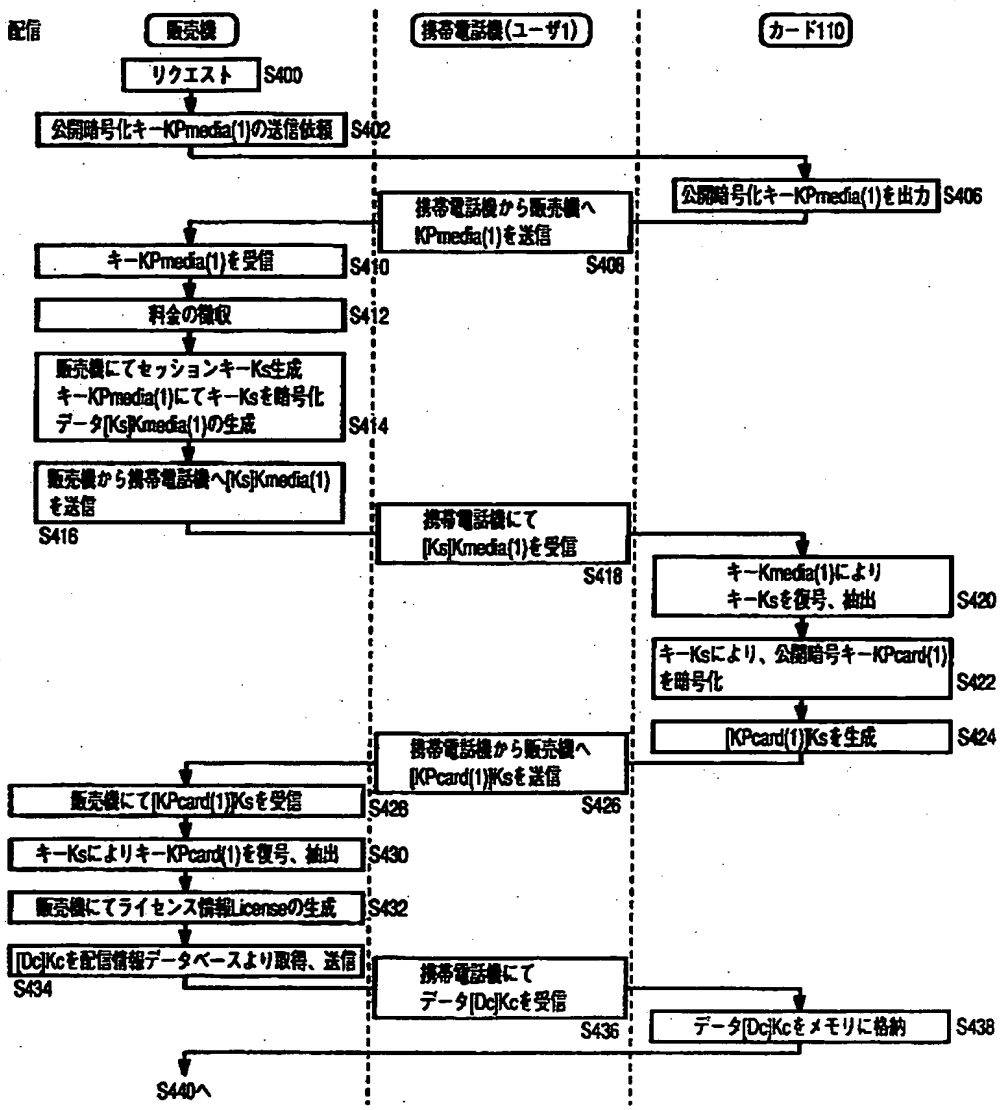
【図２０】



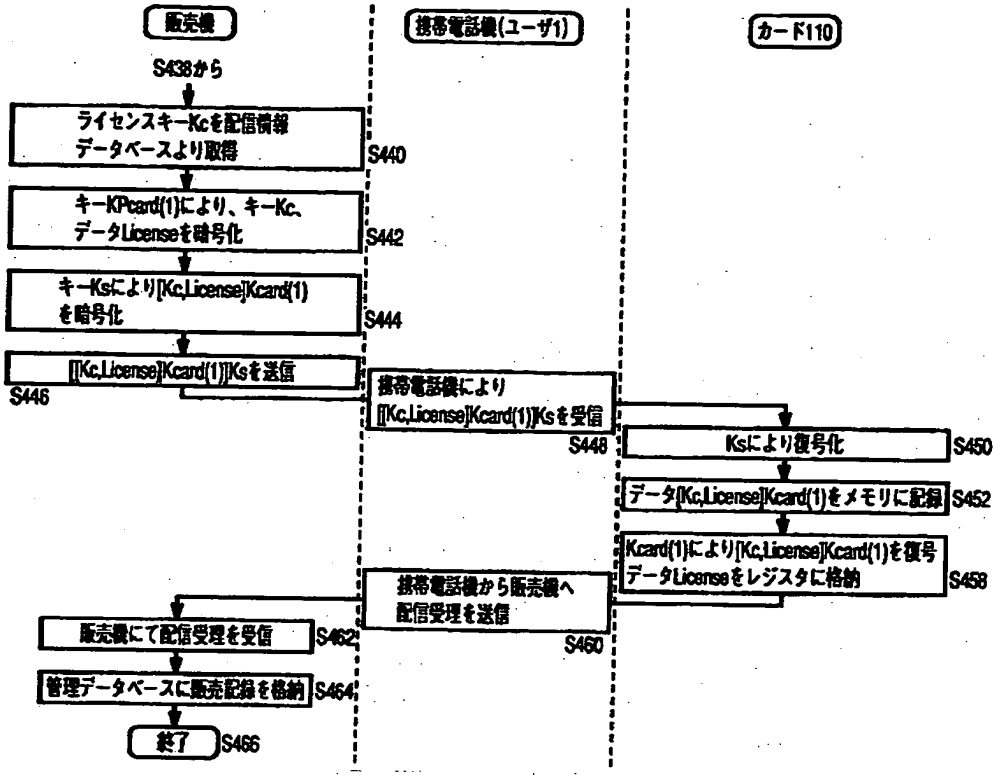
【図２１】


管理サーバ
2200
2000
配信情報データベース
304
送受信
360
2100
配信制御
暗号化
320
Ks発生
314
312
BS1
322
暗号化
318
復号
316
暗号化
ディスプレイ
2002
キーボード
2004
2012
インターフェース
2010
料金受理
2020

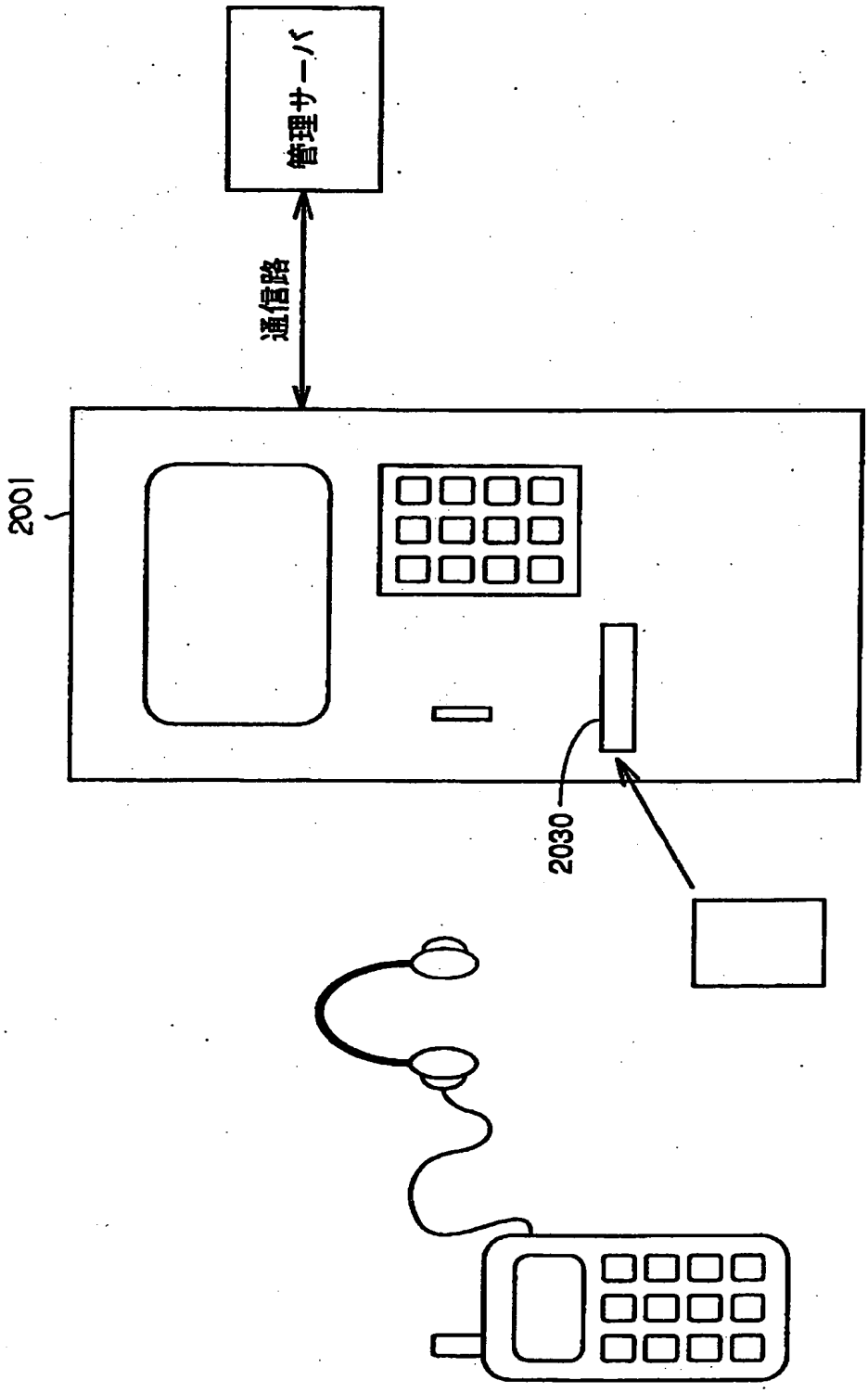
【図２２】


配信
販売機
携帯電話機(ユーザ1)
カード110
リクエスト S400
公開暗号化キーKPmedia(1)の送信依頼 S402
公開暗号化キーKPmedia(1)を出力 S406
携帯電話機から販売機へ KPmedia(1)を送信 S408
キーKPmedia(1)を受信 S410
料金の徴収 S412
販売機にてセッションキーKs生成 キーKPmedia(1)にてキーKsを暗号化 データ[Ks]Kmedia(1)の生成 S414
販売機から携帯電話機へ[Ks]Kmedia(1)を送信 S416
携帯電話機にて [Ks]Kmedia(1)を受信 S418
キーKmedia(1)により キーKsを復号、抽出 S420
キーKsにより、公開暗号キーKPcard(1)を暗号化 S422
[KPcard(1)]Ksを生成 S424
携帯電話機から販売機へ [KPcard(1)]Ksを送信 S426
販売機にて[KPcard(1)]Ksを受信 S428
キーKsによりキーKPcard(1)を復号、抽出 S430
販売機にてライセンス情報Licenseの生成 S432
[Dc]Kcを配信情報データベースより取得、送信 S434
携帯電話機にて データ[Dc]Kcを受信 S436
データ[Dc]Kcをメモリに格納 S438
S440へ

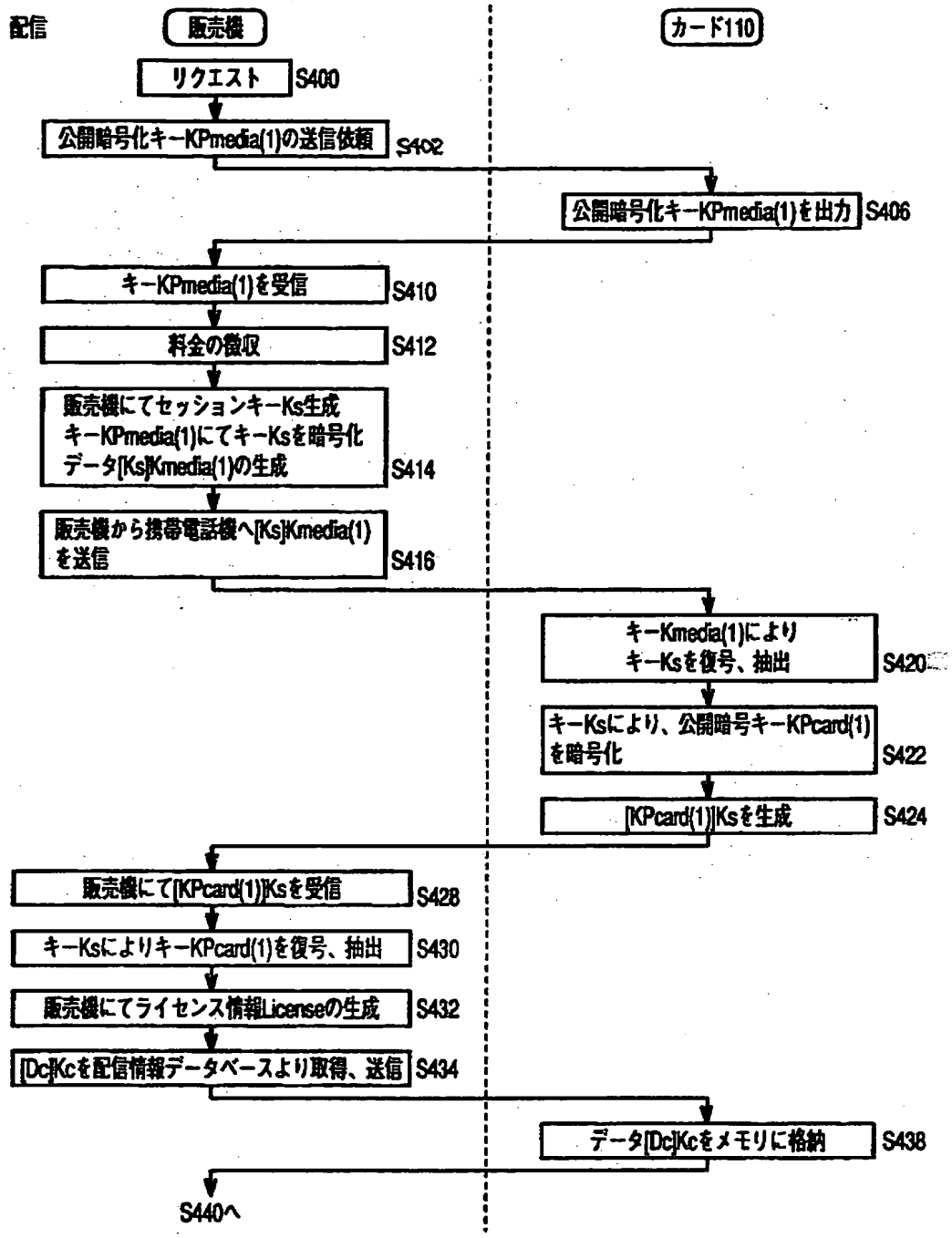
【図２３】


販売機
携帯電話機(ユーザ1)
カード110
S438から
ライセンスキーKcを配信情報データベースより取得
S440
キーKPcard(1)により、キーKc、データLicenseを暗号化
S442
キーKsにより[Kc,License]Kcard(1)を暗号化
S444
[[Kc,License]Kcard(1)]Ksを送信
S446
携帯電話機により[[Kc,License]Kcard(1)]Ksを受信
S448
Ksにより復号化
S450
データ[Kc,License]Kcard(1)をメモリに記録
S452
Kcard(1)により[Kc,License]Kcard(1)を復号データLicenseをレジスタに格納
S458
携帯電話機から販売機へ配信受理を送信
S460
販売機にて配信受理を受信
S462
管理データベースに販売記録を格納
S464
終了
S466

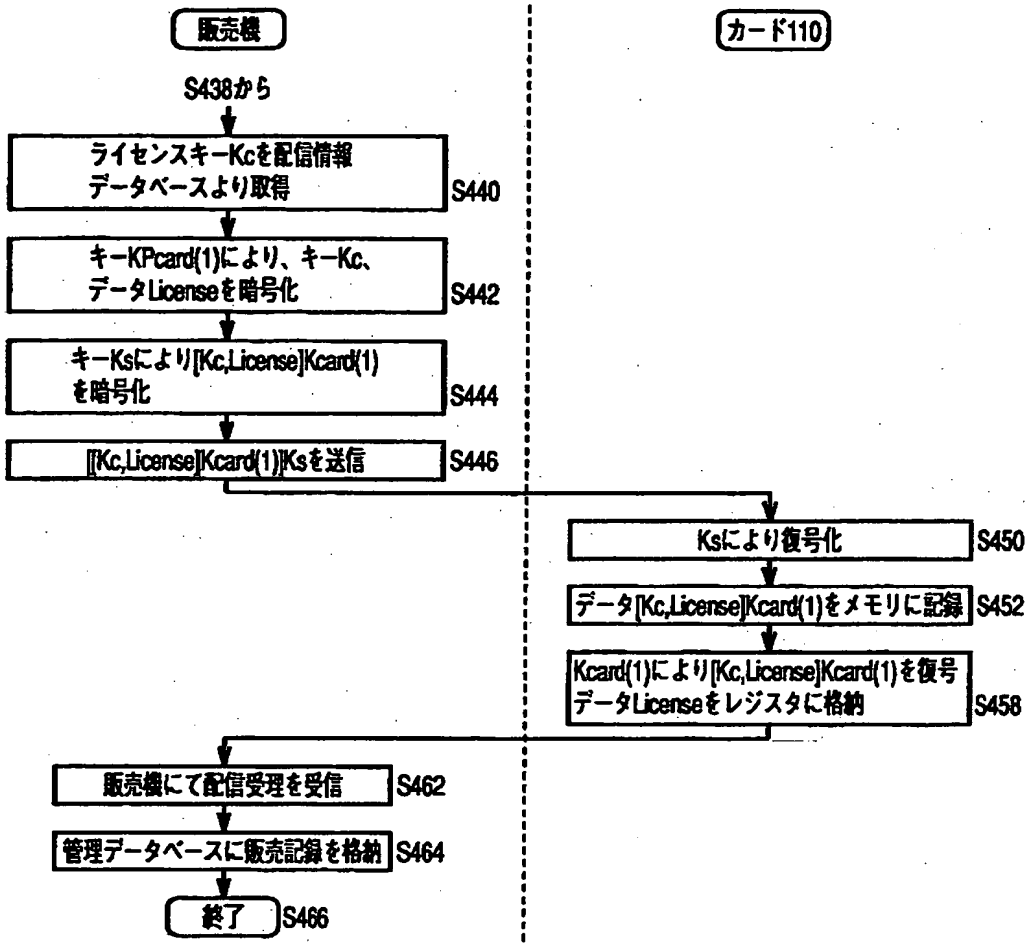
【図２４】



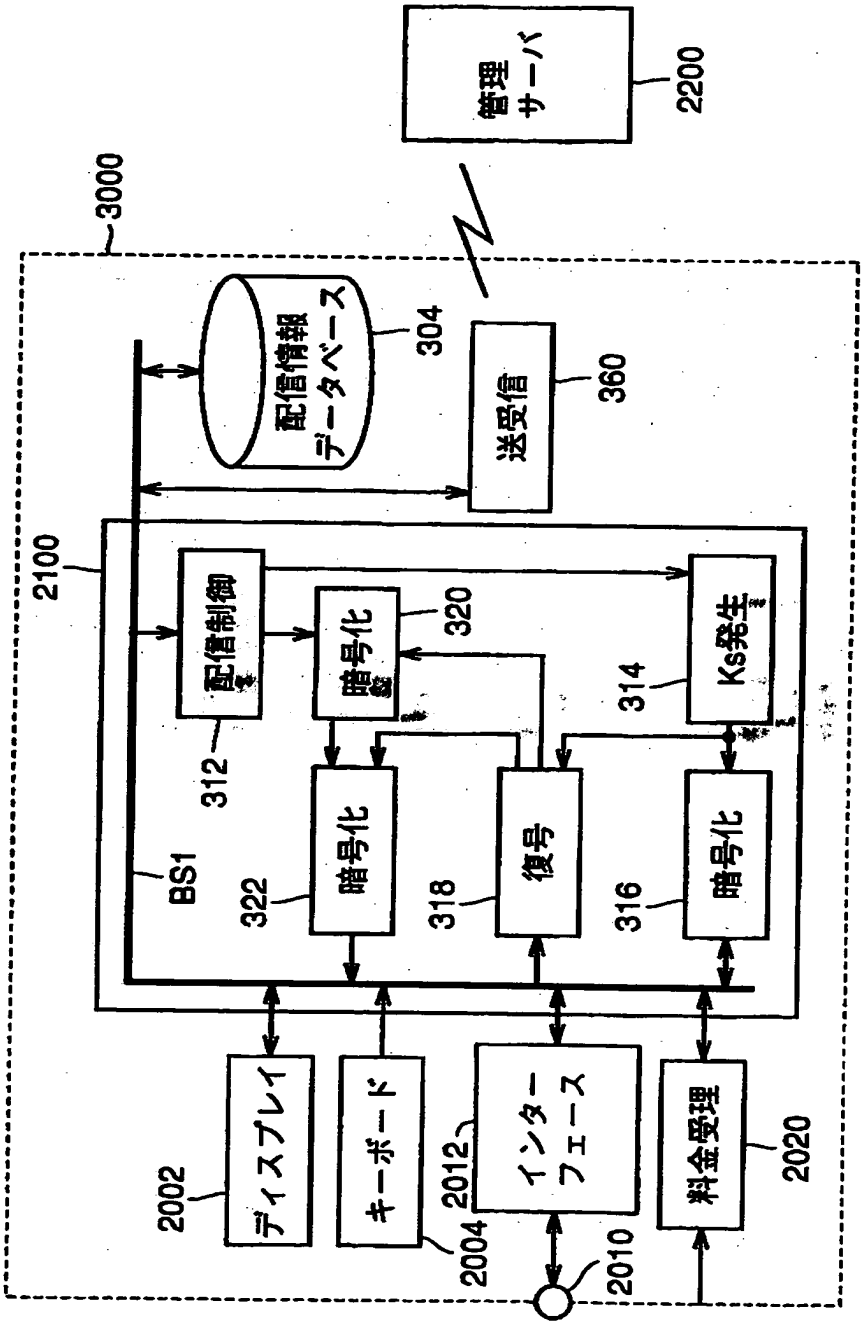
【図２５】


配信
販売機
カード110
リクエスト S400
公開暗号化キーKPmedia(1)の送信依頼 S402
公開暗号化キーKPmedia(1)を出力 S406
キーKPmedia(1)を受信 S410
料金の徴収 S412
販売機にてセッションキーKs生成
キーKPmedia(1)にてキーKsを暗号化
データ[Ks]Kmedia(1)の生成 S414
販売機から携帯電話機へ[Ks]Kmedia(1)
を送信 S416
キーKmedia(1)により
キーKsを復号、抽出 S420
キーKsにより、公開暗号キーKPcard(1)
を暗号化 S422
[KPcard(1)]Ksを生成 S424
販売機にて[KPcard(1)]Ksを受信 S428
キーKsによりキーKPcard(1)を復号、抽出 S430
販売機にてライセンス情報Licenseの生成 S432
[Dc]Kcを配信情報データベースより取得、送信 S434
データ[Dc]Kcをメモリに格納 S438
S440へ

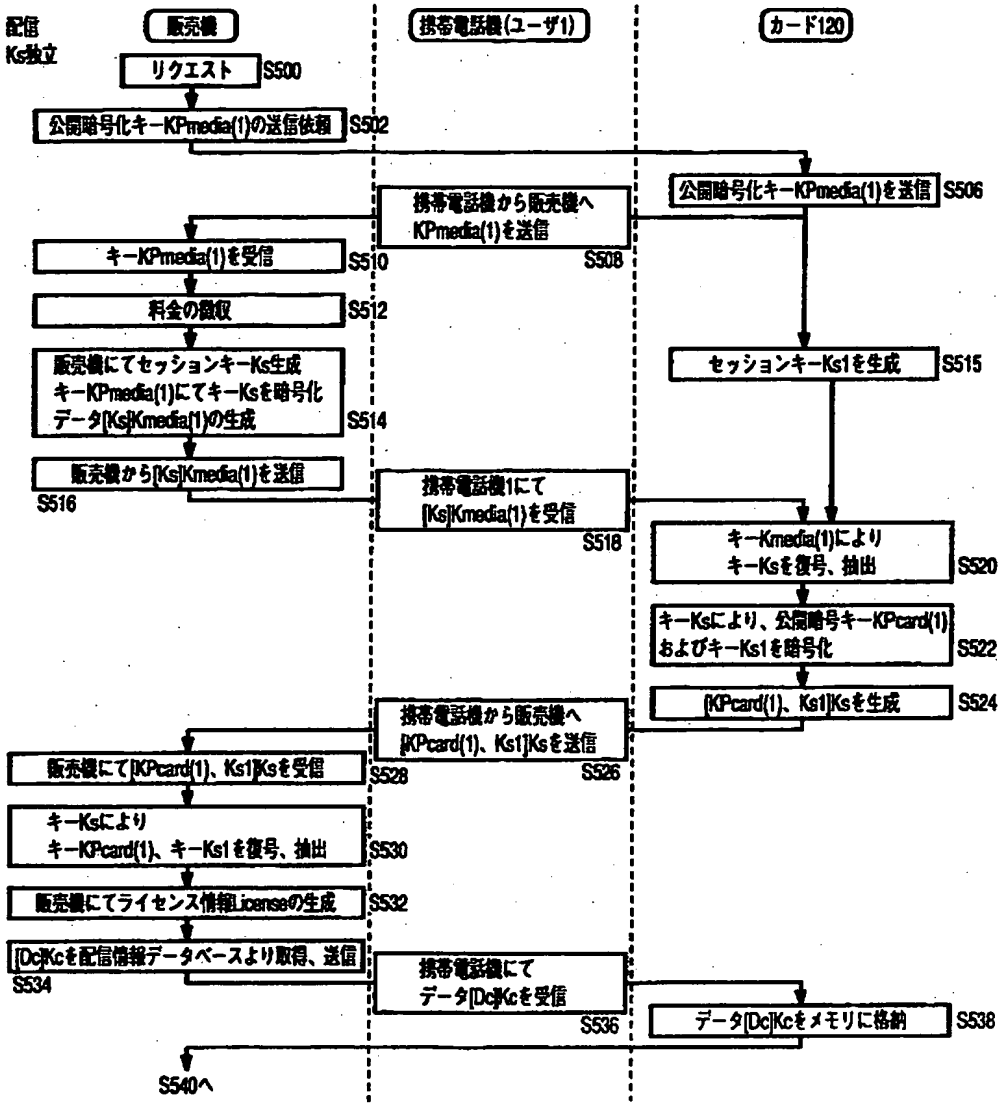
【図２６】


販売機
カード110
S438から
ライセンスキーKcを配信情報データベースより取得
S440
キーKPcard(1)により、キーKc、データLicenseを暗号化
S442
キーKsにより[Kc,License]Kcard(1)を暗号化
S444
[Kc,License]Kcard(1)Ksを送信
S446
Ksにより復号化
S450
データ[Kc,License]Kcard(1)をメモリに記録
S452
Kcard(1)により[Kc,License]Kcard(1)を復号データLicenseをレジスタに格納
S458
販売機にて配信受理を受信
S462
管理データベースに販売記録を格納
S464
終了
S466

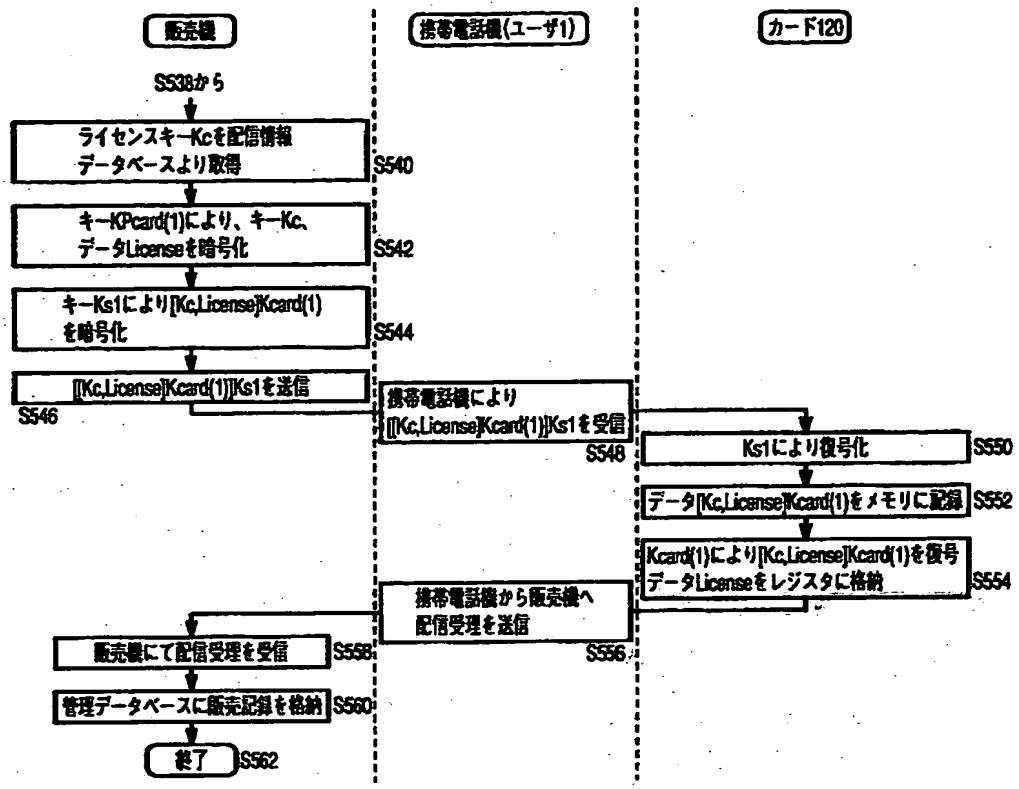
【図２７】


管理サーバ
2200
3000
配信情報データベース
304
送受信
360
2100
配信制御
312
暗号化
320
Ks発生
314
BS1
暗号化
322
復号
318
暗号化
316
ディスプレイ
2002
キーボード
2004
インターフェース
2012
料金受理
2020
2010

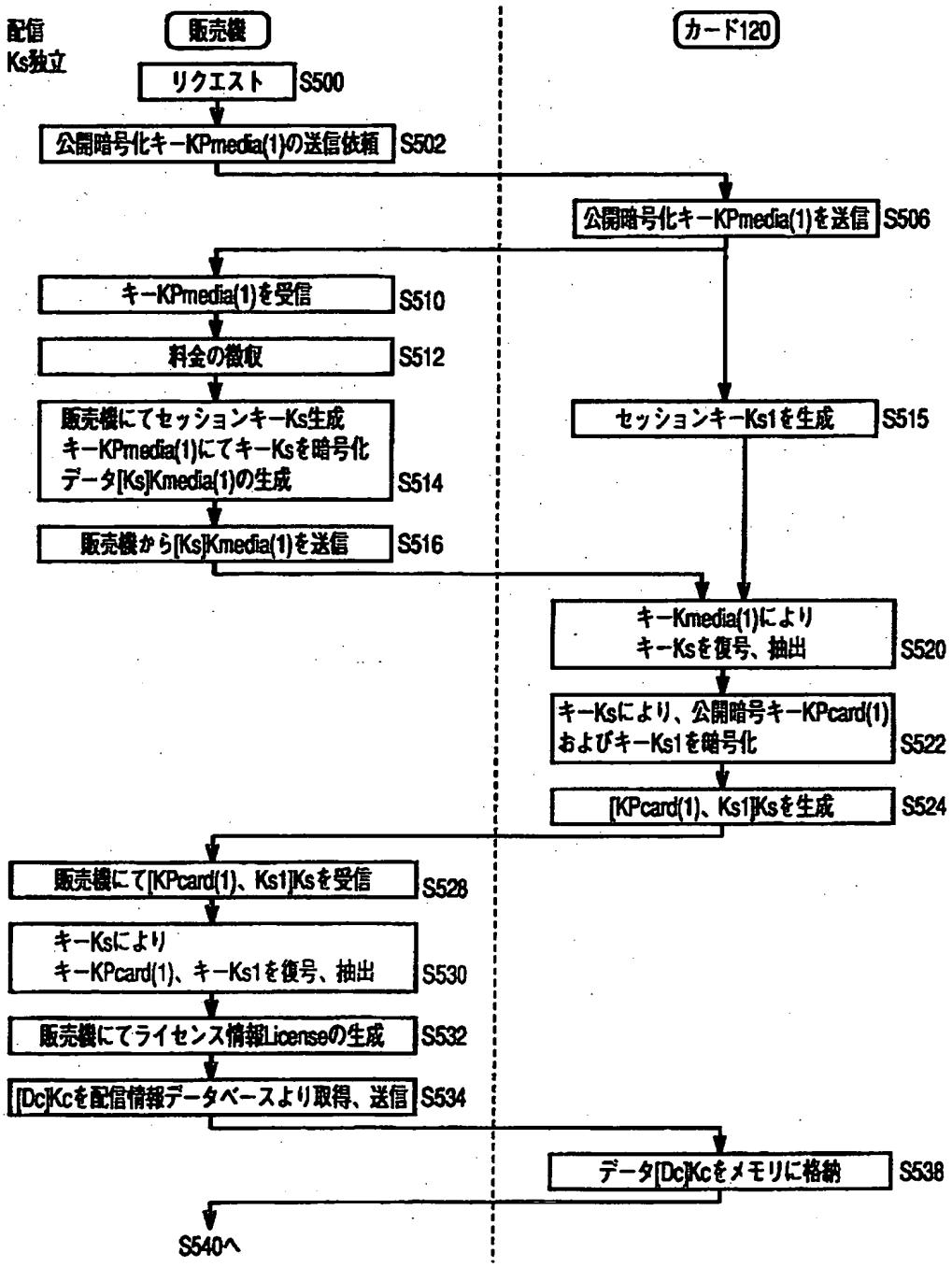
【図２８】


配信
Ks独立
販売機
携帯電話機(ユーザ1)
カード120
リクエスト S500
公開暗号化キーKPmedia(1)の送信依頼 S502
公開暗号化キーKPmedia(1)を送信 S506
携帯電話機から販売機へ
KPmedia(1)を送信 S508
キーKPmedia(1)を受信 S510
料金の徴収 S512
セッションキーKs1を生成 S515
販売機にてセッションキーKs生成
キーKPmedia(1)にてキーKsを暗号化
データ[Ks]Kmedia(1)の生成 S514
販売機から[Ks]Kmedia(1)を送信 S516
携帯電話機1にて
[Ks]Kmedia(1)を受信 S518
キーKmedia(1)により
キーKsを復号、抽出 S520
キーKsにより、公開暗号キーKPcard(1)
およびキーKs1を暗号化 S522
[KPcard(1)、Ks1]Ksを生成 S524
携帯電話機から販売機へ
[KPcard(1)、Ks1]Ksを送信 S526
販売機にて[KPcard(1)、Ks1]Ksを受信 S528
キーKsにより
キーKPcard(1)、キーKs1を復号、抽出 S530
販売機にてライセンス情報Licenseの生成 S532
[Dc]Kcを配信情報データベースより取得、送信 S534
携帯電話機にて
データ[Dc]Kcを受信 S536
データ[Dc]Kcをメモリに格納 S538
S540へ

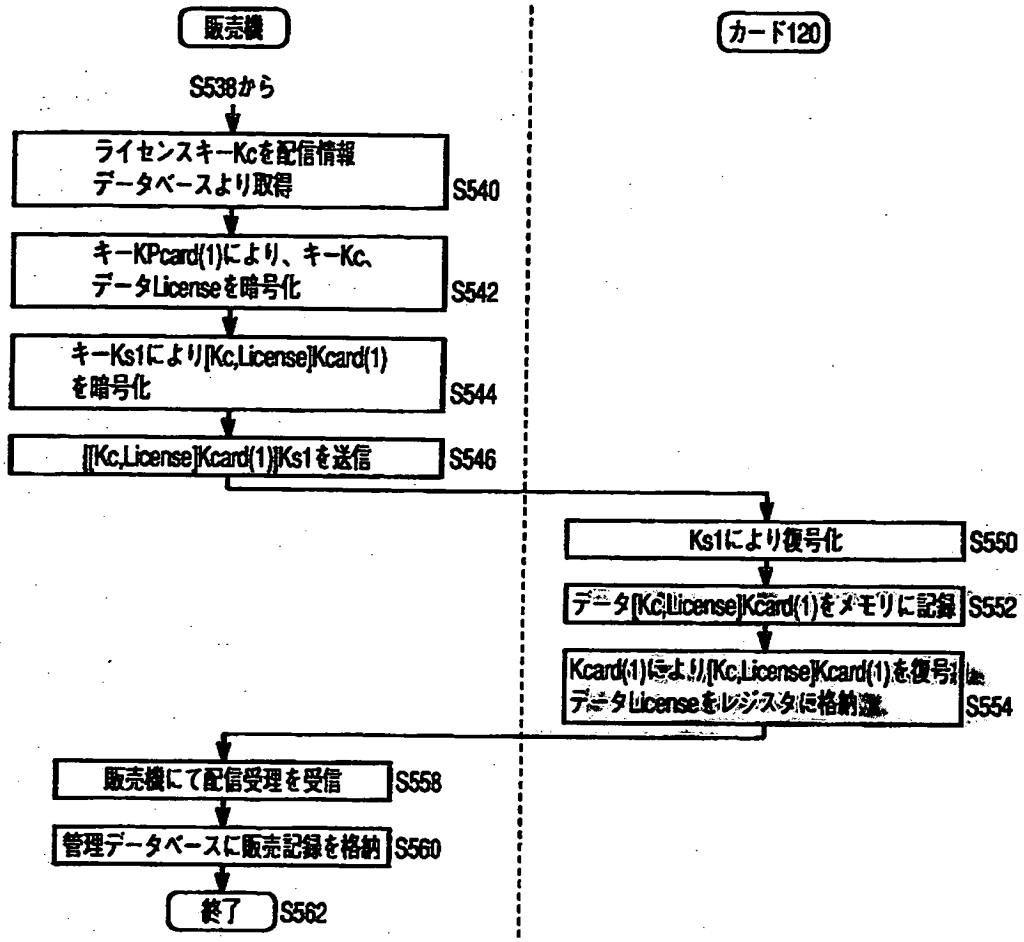
【図２９】


販売機
携帯電話機(ユーザ1)
カード120
S538から
ライセンスキーKcを配信情報データベースより取得
S540
キーKPcard(1)により、キーKc、データLicenseを暗号化
S542
キーKs1により[Kc,License]Kcard(1)を暗号化
S544
[[Kc,License]Kcard(1)]Ks1を送信
S546
携帯電話機により[[Kc,License]Kcard(1)]Ks1を受信
S548
Ks1により復号化
S550
データ[Kc,License]Kcard(1)をメモリに記録
S552
Kcard(1)により[Kc,License]Kcard(1)を復号データLicenseをレジスタに格納
S554
携帯電話機から販売機へ配信受理を送信
S556
販売機にて配信受理を受信
S558
管理データベースに販売記録を格納
S560
終了
S562

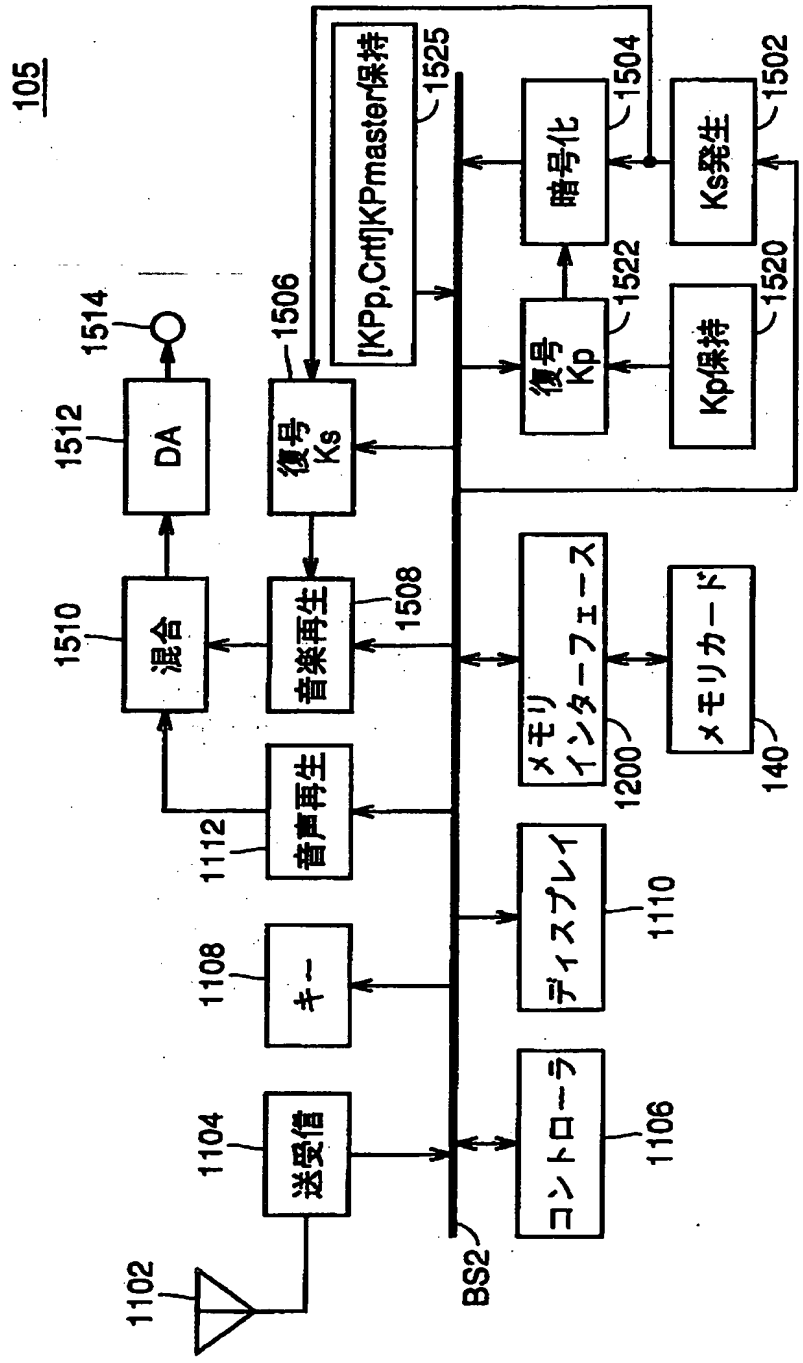
【図３０】


配信
Ks独立
販売機
カード120
リクエスト S500
公開暗号化キーKPmedia(1)の送信依頼 S502
公開暗号化キーKPmedia(1)を送信 S506
キーKPmedia(1)を受信 S510
料金の徴収 S512
販売機にてセッションキーKs生成
キーKPmedia(1)にてキーKsを暗号化
データ[Ks]Kmedia(1)の生成 S514
セッションキーKs1を生成 S515
販売機から[Ks]Kmedia(1)を送信 S516
キーKmedia(1)により
キーKsを復号、抽出 S520
キーKsにより、公開暗号キーKPcard(1)
およびキーKs1を暗号化 S522
[KPcard(1)、Ks1]Ksを生成 S524
販売機にて[KPcard(1)、Ks1]Ksを受信 S528
キーKsにより
キーKPcard(1)、キーKs1を復号、抽出 S530
販売機にてライセンス情報Licenseの生成 S532
[Dc]Kcを配信情報データベースより取得、送信 S534
データ[Dc]Kcをメモリに格納 S538
S540へ

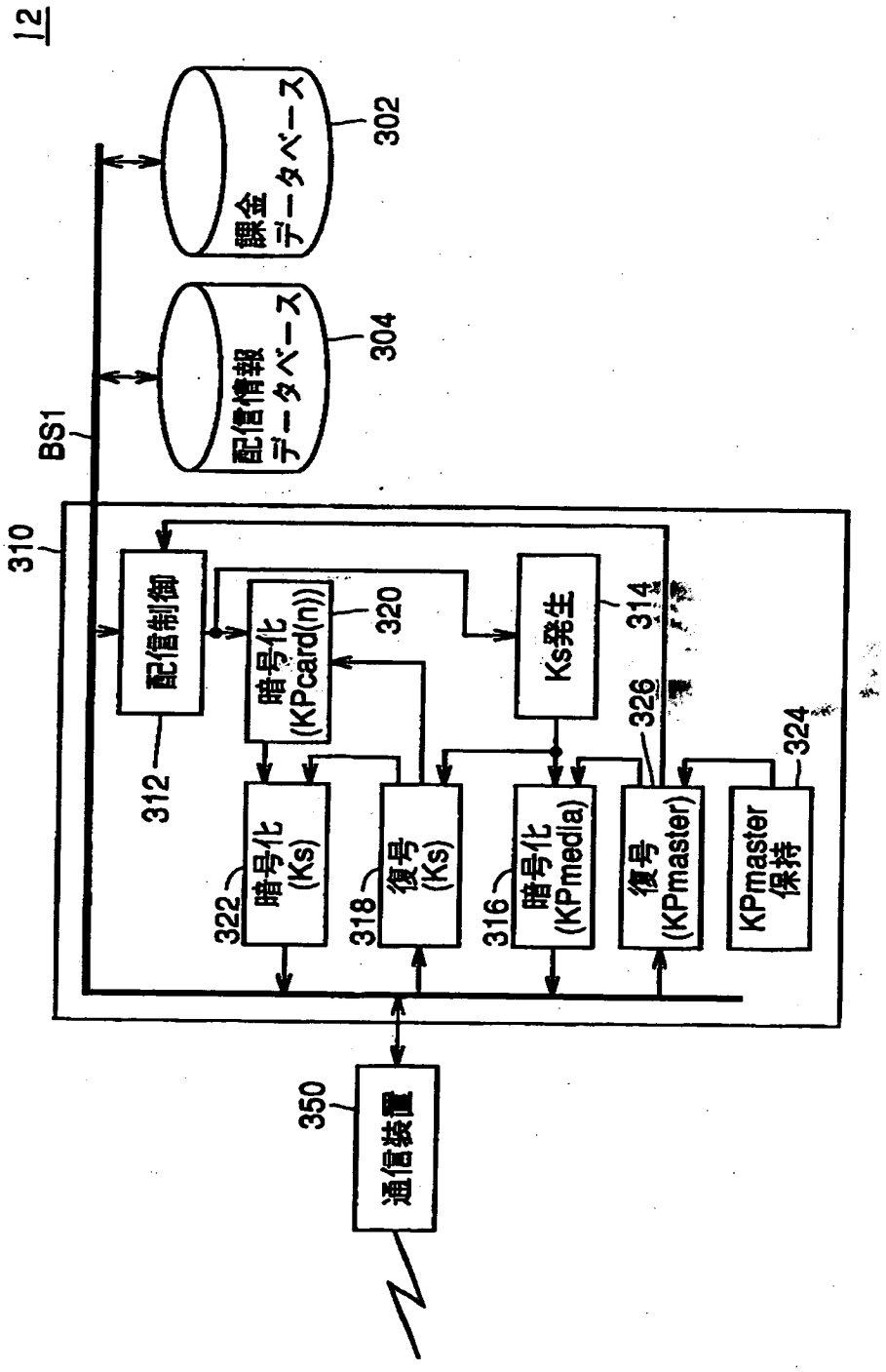
【図３１】


販売機
カード120
S538から
ライセンスキーKcを配信情報データベースより取得
S540
キーKPcard(1)により、キーKc、データLicenseを暗号化
S542
キーKs1により[Kc,License]Kcard(1)を暗号化
S544
[[Kc,License]Kcard(1)]Ks1を送信
S546
Ks1により復号化
S550
データ[Kc,License]Kcard(1)をメモリに記録
S552
Kcard(1)により[Kc,License]Kcard(1)を復号し、データLicenseをレジスタに格納
S554
販売機にて配信受理を受信
S558
管理データベースに販売記録を格納
S560
終了
S562

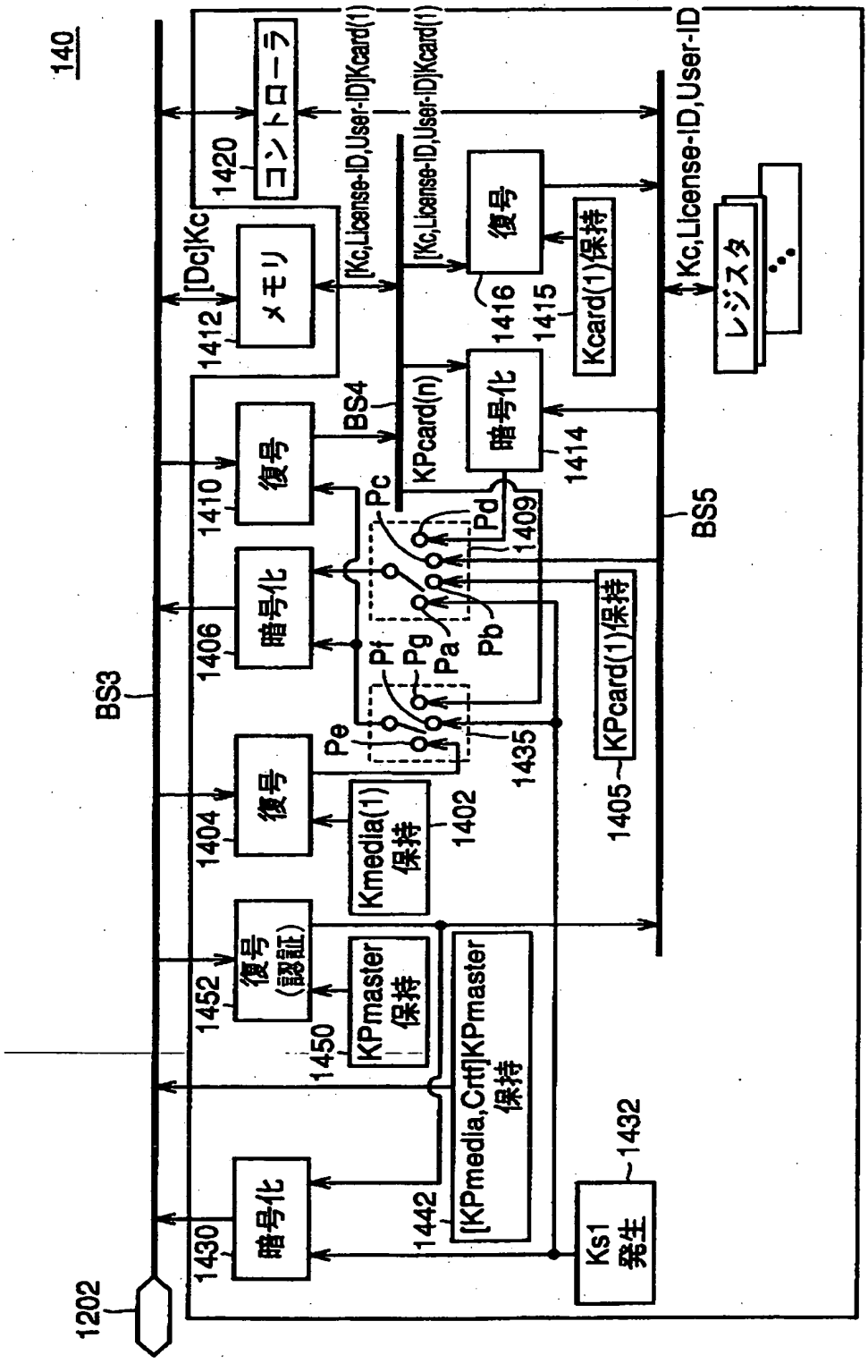
【図３２】


105
1514
1512
DA
1510
混合
1102
1104
送受信
1108
キー
1112
音声再生
1506
復号 Ks
1508
音楽再生
[KPp,Cnt]KPmaster保持
1525
BS2
コントローラ
1106
ディスプレイ
1110
メモリ インターフェース
1200
メモリカード
140
暗号化
1504
復号 Kp
1522
Kp保持
1520
Ks発生
1502

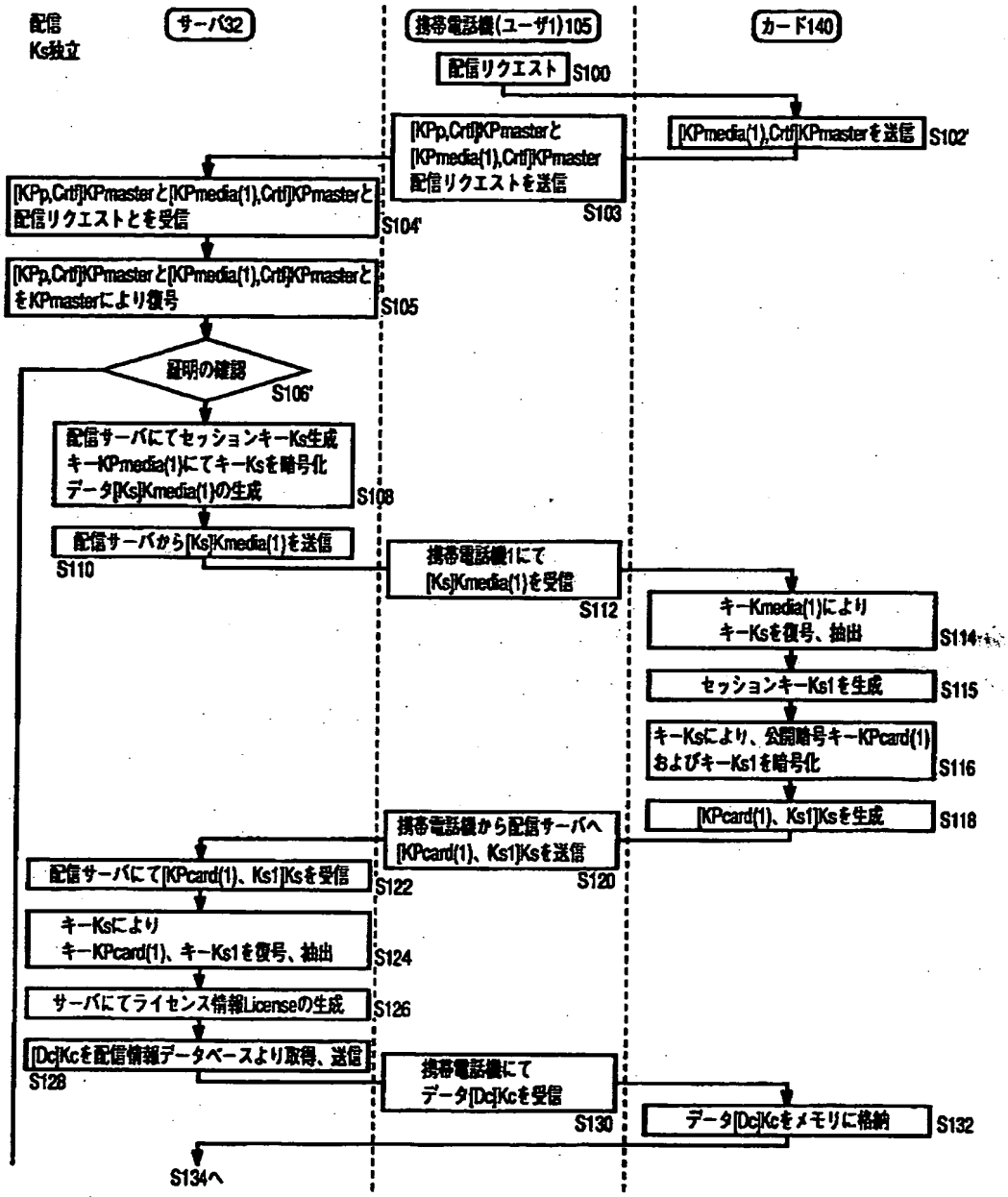
【図３３】


12
課金データベース
302
配信情報データベース
304
BS1
310
配信制御
312
暗号化(KPcard(n))
320
Ks発生
314
326
324
暗号化(Ks)
322
復号(Ks)
318
暗号化(KPmedia)
316
復号(KPmaster)
KPmaster保持
350
通信装置

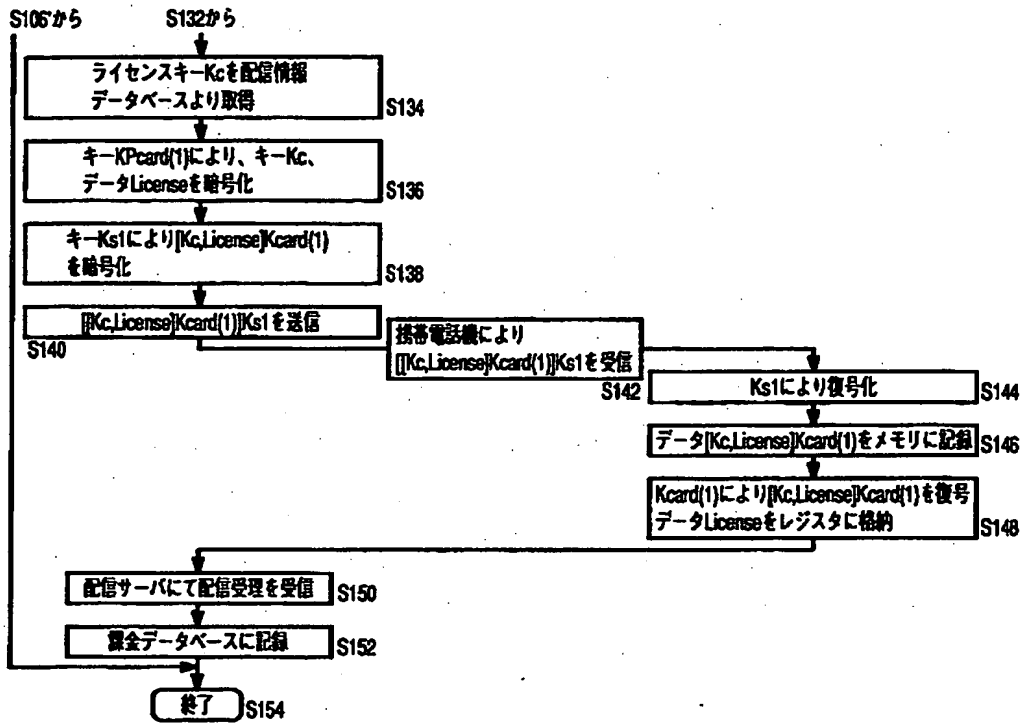
【図３４】


140
コントローラ
1420
メモリ
1412
[Dc]Kc
[Kc,License-ID,User-ID]Kcard(1)
[Kc,License-ID,User-ID]Kcard(1)
Kc,License-ID,User-ID
レジスタ
復号
1416
Kcard(1)保持
1415
暗号化
1414
KPcard(n)
BS4
BS5
復号
1410
暗号化
1406
復号
1404
復号(認証)
1452
KPmaster保持
1450
Kmedia(1)保持
1402
KPcard(1)保持
1405
1409
1435
Pc
Pd
Pe
Pf
Pg
Pa
Pb
BS3
暗号化
1430
[KPmedia,Crtf]KPmaster保持
1442
Ks1発生
1432
1202

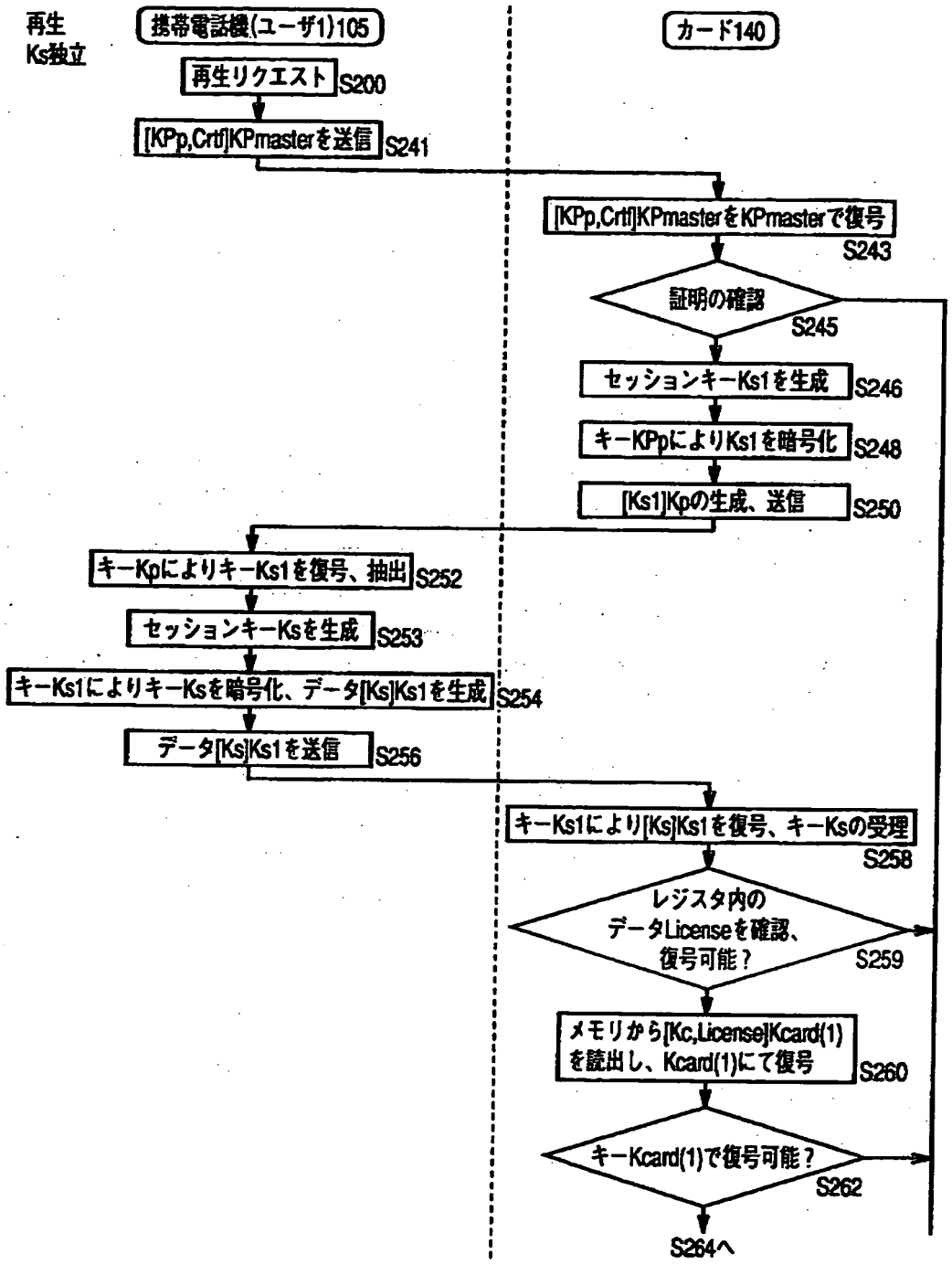
【図３５】


配信
Ks独立
サーバ32
携帯電話機(ユーザ1)105
カード140
配信リクエスト S100
[KPp,Crtf]KPmasterと
[KPmedia(1),Crtf]KPmaster
配信リクエストを送信 S103
[KPmedia(1),Crtf]KPmasterを送信 S102'
[KPp,Crtf]KPmasterと[KPmedia(1),Crtf]KPmasterと
配信リクエストとを受信 S104'
[KPp,Crtf]KPmasterと[KPmedia(1),Crtf]KPmasterと
をKPmasterにより復号 S105
証明の確認 S106'
配信サーバにてセッションキーKs生成
キーKPmedia(1)にてキーKsを暗号化
データ[Ks]Kmedia(1)の生成 S108
配信サーバから[Ks]Kmedia(1)を送信
S110
携帯電話機1にて
[Ks]Kmedia(1)を受信 S112
キーKmedia(1)により
キーKsを復号、抽出 S114
セッションキーKs1を生成 S115
キーKsにより、公開暗号キーKPcard(1)
およびキーKs1を暗号化 S116
[KPcard(1)、Ks1]Ksを生成 S118
携帯電話機から配信サーバへ
[KPcard(1)、Ks1]Ksを送信 S120
配信サーバにて[KPcard(1)、Ks1]Ksを受信
S122
キーKsにより
キーKPcard(1)、キーKs1を復号、抽出 S124
サーバにてライセンス情報Licenseの生成 S126
[Dc]Kcを配信情報データベースより取得、送信
S128
携帯電話機にて
データ[Dc]Kcを受信 S130
データ[Dc]Kcをメモリに格納 S132
S134へ

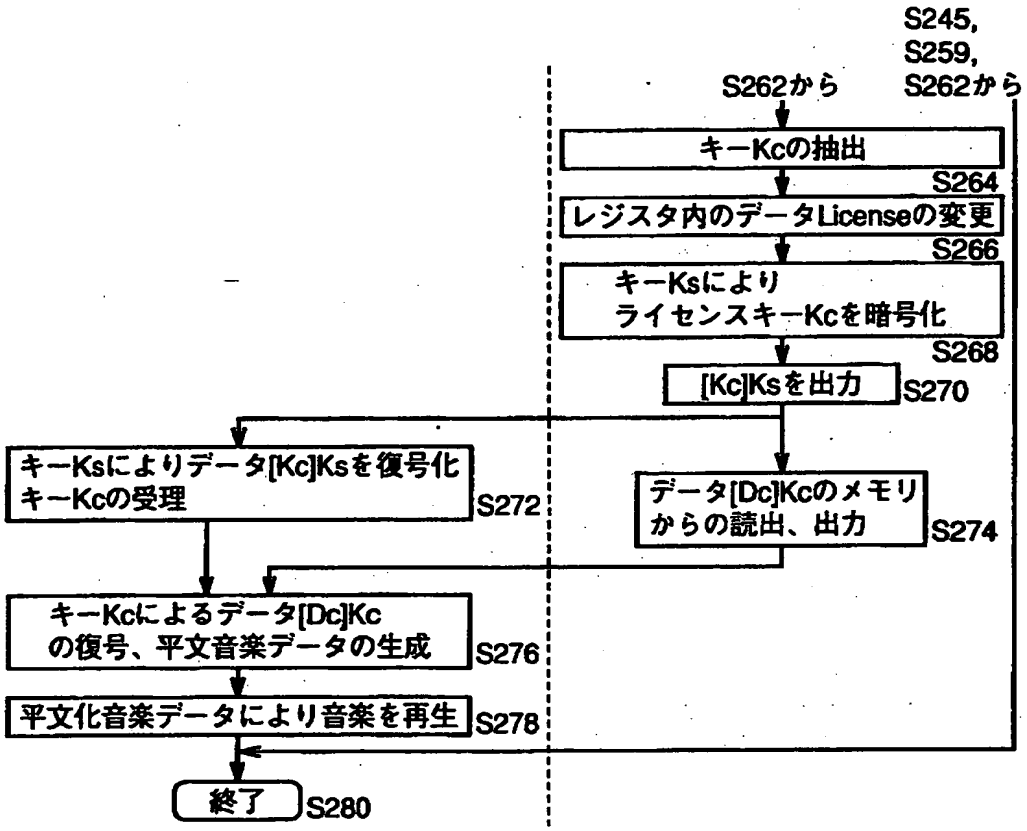
【図３６】


S105から
S132から
ライセンスキーKcを配信情報データベースより取得
S134
キーKPcard(1)により、キーKc、データLicenseを暗号化
S136
キーKs1により[Kc,License]Kcard(1)を暗号化
S138
[[Kc,License]Kcard(1)]Ks1を送信
S140
携帯電話機により[[Kc,License]Kcard(1)]Ks1を受信
S142
Ks1により復号化
S144
データ[Kc,License]Kcard(1)をメモリに記録
S146
Kcard(1)により[Kc,License]Kcard(1)を復号データLicenseをレジスタに格納
S148
配信サーバにて配信受理を受信
S150
課金データベースに記録
S152
終了
S154

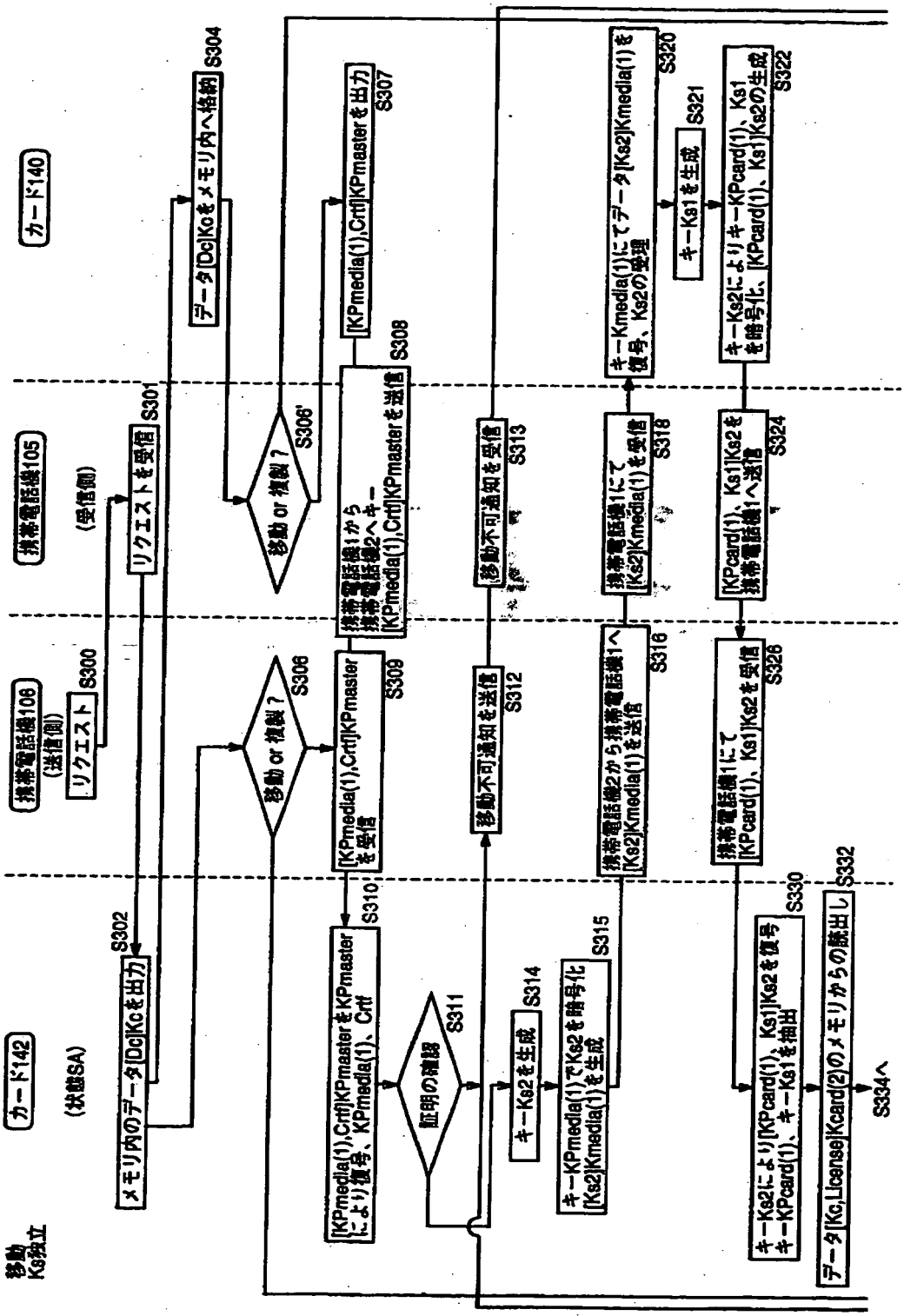
【図３７】


再生
Ks独立
携帯電話機(ユーザ1)105
カード140
再生リクエスト S200
[KPp,Crtf]KPmasterを送信 S241
[KPp,Crtf]KPmasterをKPmasterで復号 S243
証明の確認 S245
セッションキーKs1を生成 S246
キーKPpによりKs1を暗号化 S248
[Ks1]Kpの生成、送信 S250
キーKpによりキーKs1を復号、抽出 S252
セッションキーKsを生成 S253
キーKs1によりキーKsを暗号化、データ[Ks]Ks1を生成 S254
データ[Ks]Ks1を送信 S256
キーKs1により[Ks]Ks1を復号、キーKsの受理 S258
レジスタ内の
データLicenseを確認、
復号可能？ S259
メモリから[Kc,License]Kcard(1)
を読出し、Kcard(1)にて復号 S260
キーKcard(1)で復号可能？ S262
S264へ

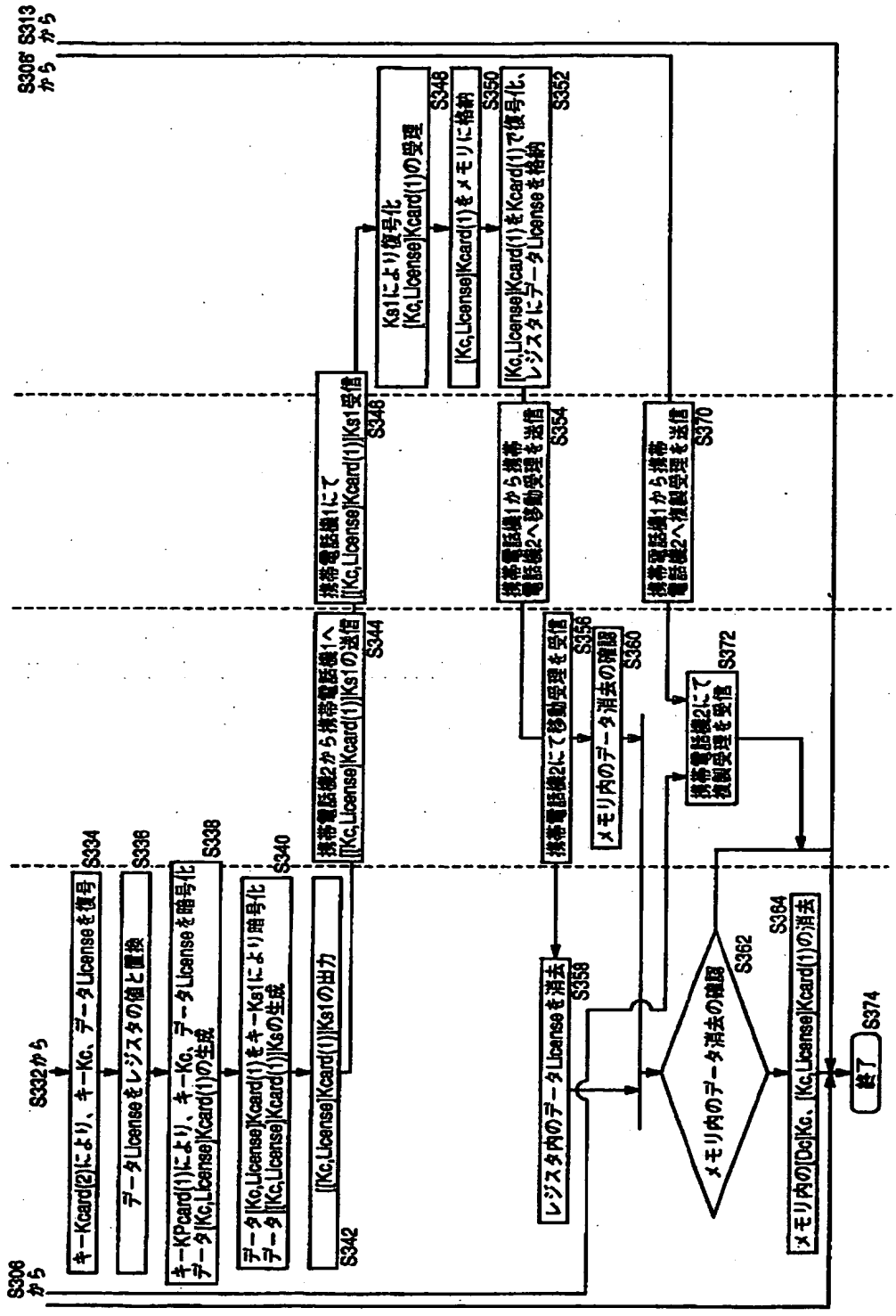
【図３８】


S245,
S259,
S262から
S262から
キーKcの抽出
S264
レジスタ内のデータLicenseの変更
S266
キーKsにより
ライセンスキーKcを暗号化
S268
[Kc]Ksを出力
S270
キーKsによりデータ[Kc]Ksを復号化
キーKcの受理
S272
データ[Dc]Kcのメモリ
からの読出、出力
S274
キーKcによるデータ[Dc]Kc
の復号、平文音楽データの生成
S276
平文化音楽データにより音楽を再生
S278
終了
S280

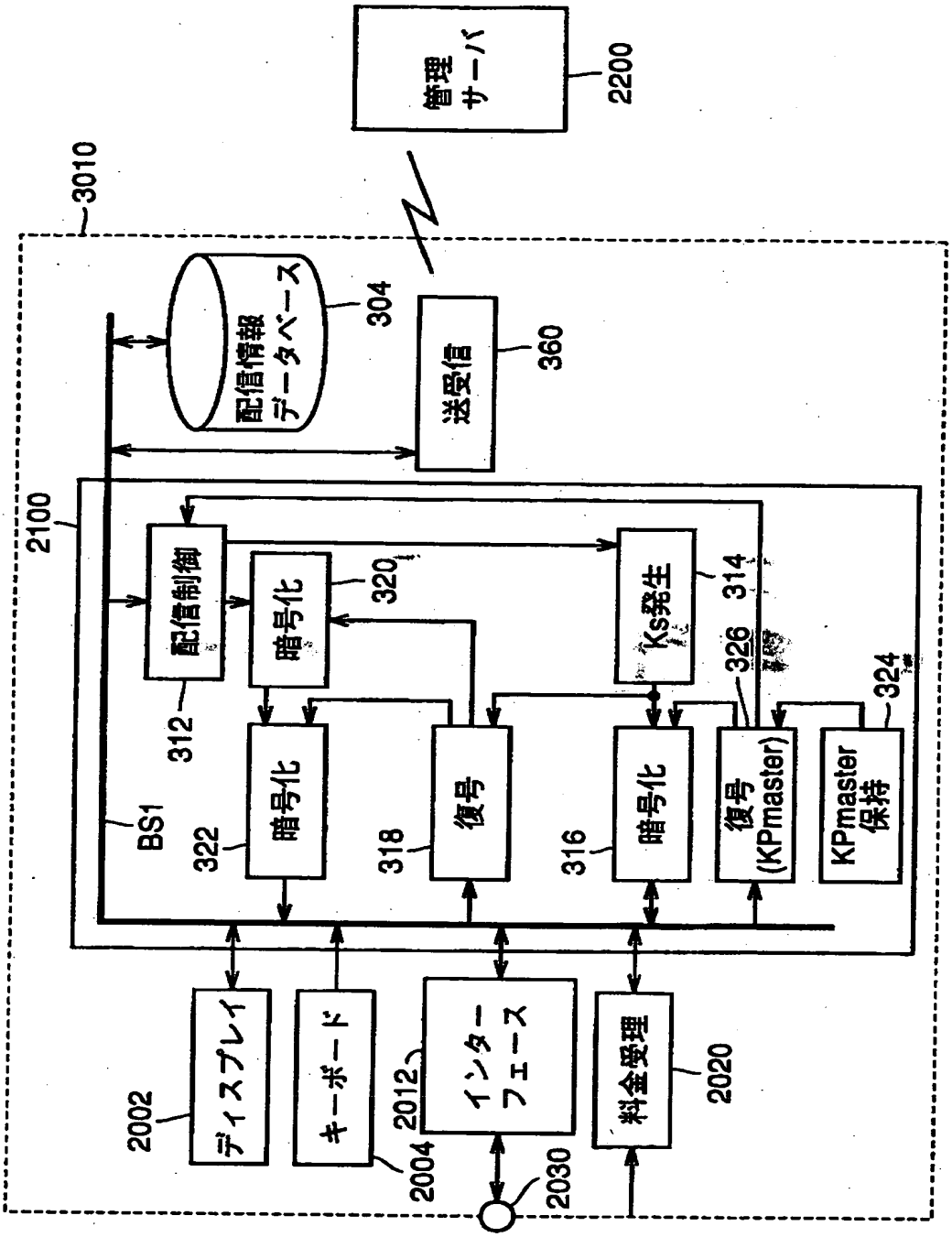
【図３９】


移動
Ks独立
カード142
(状態SA)
携帯電話機106
(送信側)
カード140
携帯電話機105
(受信側)
リクエスト
S300
メモリ内のデータ[Dc]Kcを出力
S302
リクエストを受信
S301
データ[Dc]Kcをメモリ内へ格納
S304
移動 or 複製 ?
S306
移動 or 複製 ?
S306'
[KPmedia(1),Crtf]KPmasterを出力
S307
携帯電話機1から
携帯電話機2へキー
[KPmedia(1),Crtf]KPmasterを送信
S308
[KPmedia(1),Crtf]KPmaster
を受信
S309
[KPmedia(1),Crtf]KPmasterを
により復号、KPmedia(1)、Crtf
S310
正明の確認
S311
移動不可通知を送信
S312
移動不可通知を受信
S313
キーKs2を生成
S314
キーKPmedia(1)でKs2を暗号化
[Ks2]Kmedia(1)を生成
S315
携帯電話機2から携帯電話機1へ
[Ks2]Kmedia(1)を送信
S316
携帯電話機1にて
[Ks2]Kmedia(1)を受信
S318
キーKmedia(1)にてデータ[Ks2]Kmedia(1)を
復号、Ks2の整理
S320
キーKs1を生成
S321
キーKs2によりキーKPcard(1)、Ks1
を暗号化、[KPcard(1)、Ks1]Ks2の生成
S322
[KPcard(1)、Ks1]Ks2を
携帯電話機1へ送信
S324
携帯電話機1にて
[KPcard(1)、Ks1]Ks2を受信
S326
キーKs2により[KPcard(1)、Ks1]Ks2を復号
キーKPcard(1)、キーKs1を抽出
S330
データ[Kc,License]Kcard(2)のメモリからの読出し
S332
S334へ

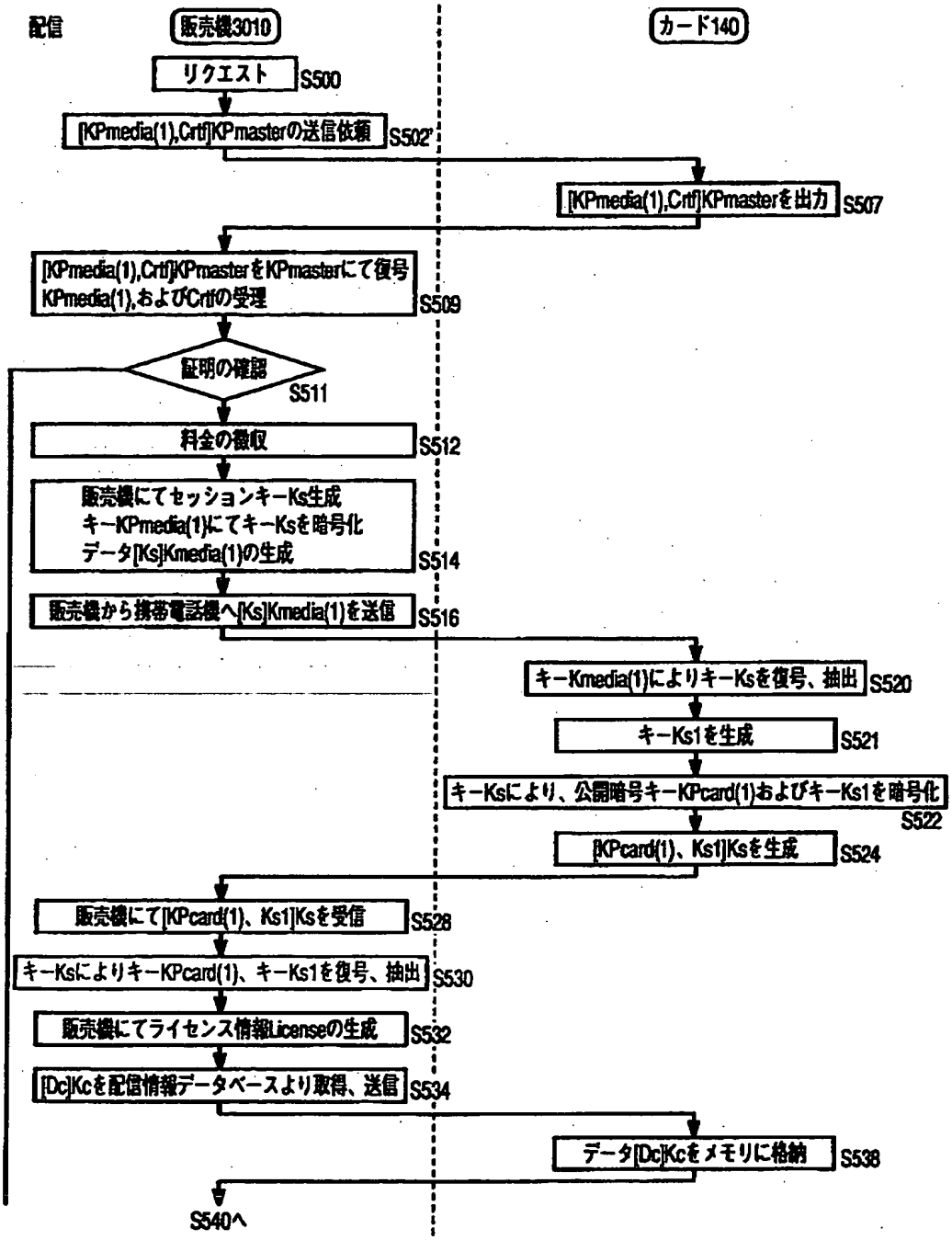
【図４０】


S306から
S332から
キーKcard(2)により、キーKc、データLicenseを復号
S334
データLicenseをレジスタの値と置換
S336
キーKPcard(1)により、キーKc、データLicenseを暗号化
データ[Kc,License]Kcard(1)の生成
S338
データ[Kc,License]Kcard(1)をキーKs1により暗号化
データ[Kc,License]Kcard(1)]Ksの生成
S340
[[Kc,License]Kcard(1)]Ks1の出力
S342
携帯電話機2から携帯電話機1へ
[[Kc,License]Kcard(1)]Ks1の送信
S344
携帯電話機1にて
[[Kc,License]Kcard(1)]Ks1受信
S346
Ks1により復号化
[Kc,License]Kcard(1)の受理
S348
[Kc,License]Kcard(1)をメモリに格納
S350
[Kc,License]Kcard(1)をKcard(1)で復号化、
レジスタにデータLicenseを格納
S352
携帯電話機1から携帯
電話機2へ移動受理を送信
S354
携帯電話機2にて移動受理を受信
S356
メモリ内のデータ消去の確認
S360
レジスタ内のデータLicenseを消去
S358
携帯電話機1から携帯
電話機2へ複製受理を送信
S370
携帯電話機2にて
複製受理を受信
S372
メモリ内のデータ消去の確認
S362
メモリ内の[Dc]Kc、[Kc,License]Kcard(1)の消去
S364
終了
S374
S306' S313
から

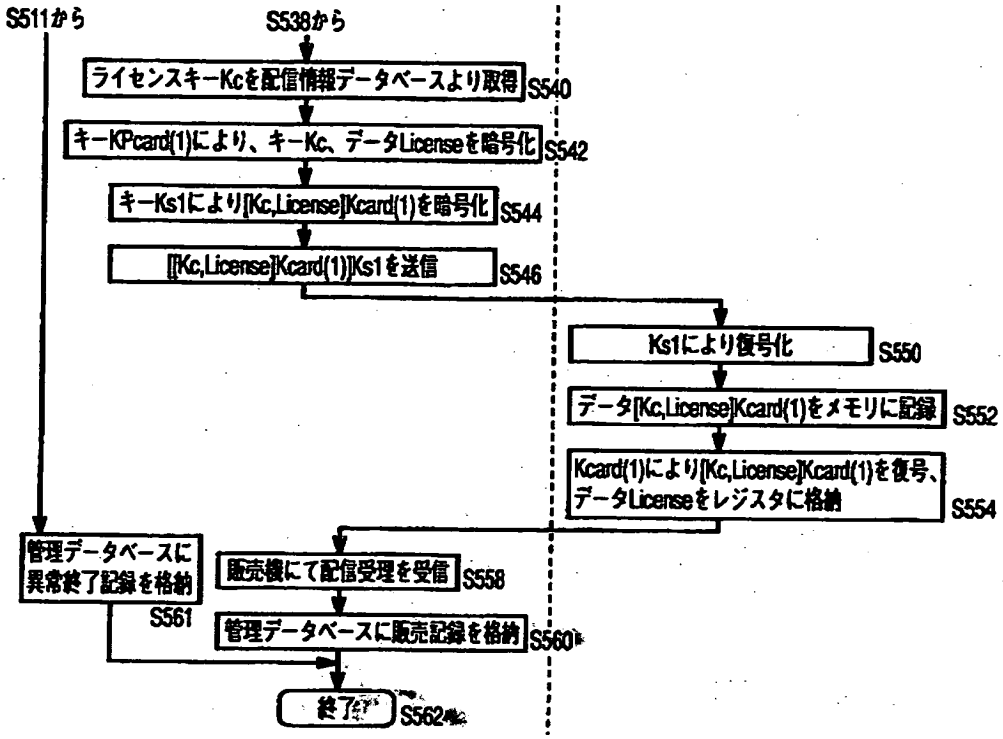
【図４１】


管理サーバ
2200
3010
配信情報データベース
304
送受信
360
2100
配信制御
312
暗号化
320
Ks発生
314
326
324
暗号化
322
復号
318
暗号化
316
復号(KPmaster)
KPmaster保持
BS1
ディスプレイ
2002
キーボード
2004
インターフェース
2012
料金受理
2020
2030

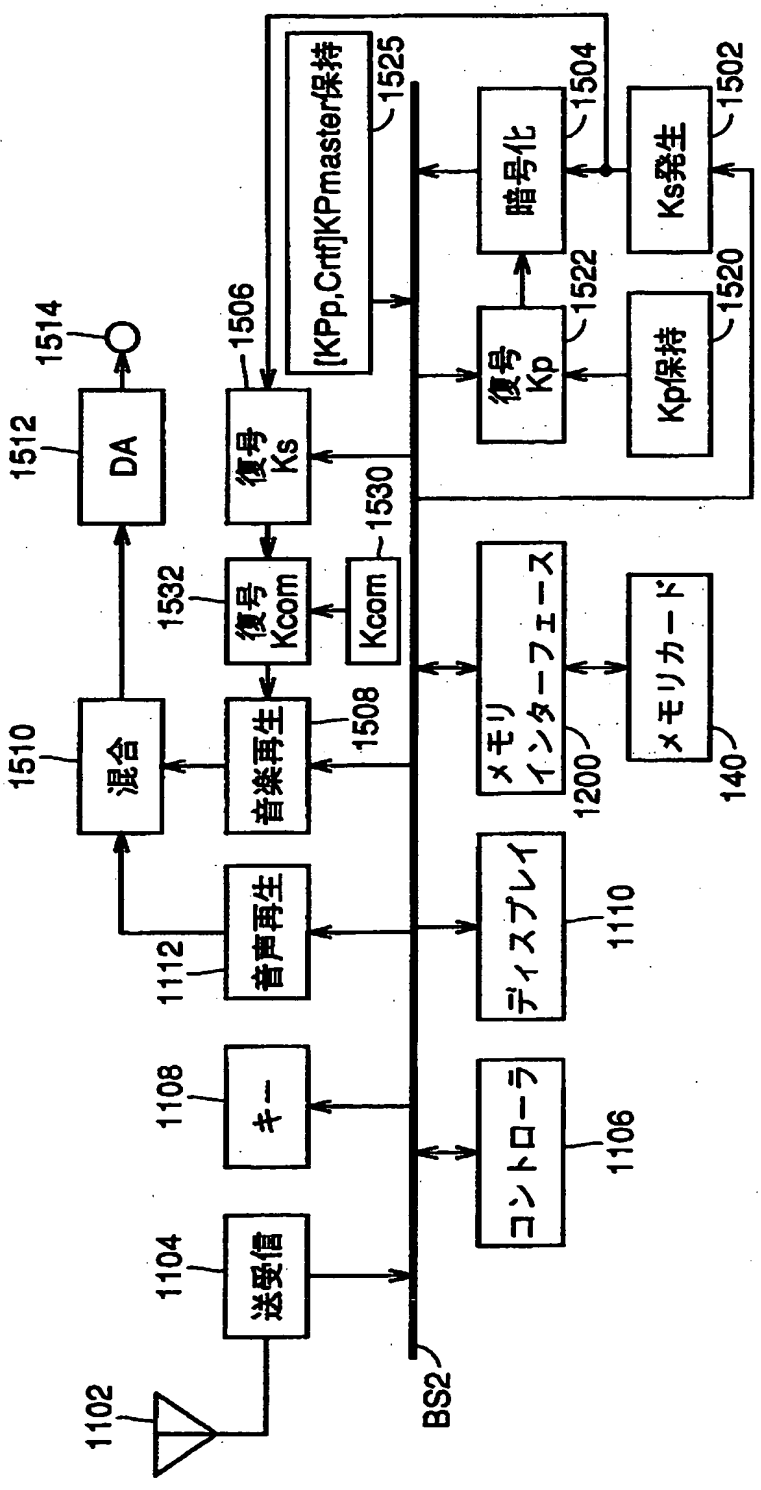
【図４２】


配信
販売機3010
カード140
リクエスト
S500
[KPmedia(1),Crtf]KPmasterの送信依頼
S502
[KPmedia(1),Crtf]KPmasterを出力
S507
[KPmedia(1),Crtf]KPmasterをKPmasterにて復号
KPmedia(1),およびCrtfの受理
S509
証明の確認
S511
料金の徴収
S512
販売機にてセッションキーKs生成
キーKPmedia(1)にてキーKsを暗号化
データ[Ks]Kmedia(1)の生成
S514
販売機から携帯電話機へ[Ks]Kmedia(1)を送信
S516
キーKmedia(1)によりキーKsを復号、抽出
S520
キーKs1を生成
S521
キーKsにより、公開暗号キーKPcard(1)およびキーKs1を暗号化
S522
[KPcard(1)、Ks1]Ksを生成
S524
販売機にて[KPcard(1)、Ks1]Ksを受信
S528
キーKsによりキーKPcard(1)、キーKs1を復号、抽出
S530
販売機にてライセンス情報Licenseの生成
S532
[Dc]Kcを配信情報データベースより取得、送信
S534
データ[Dc]Kcをメモリに格納
S538
S540へ

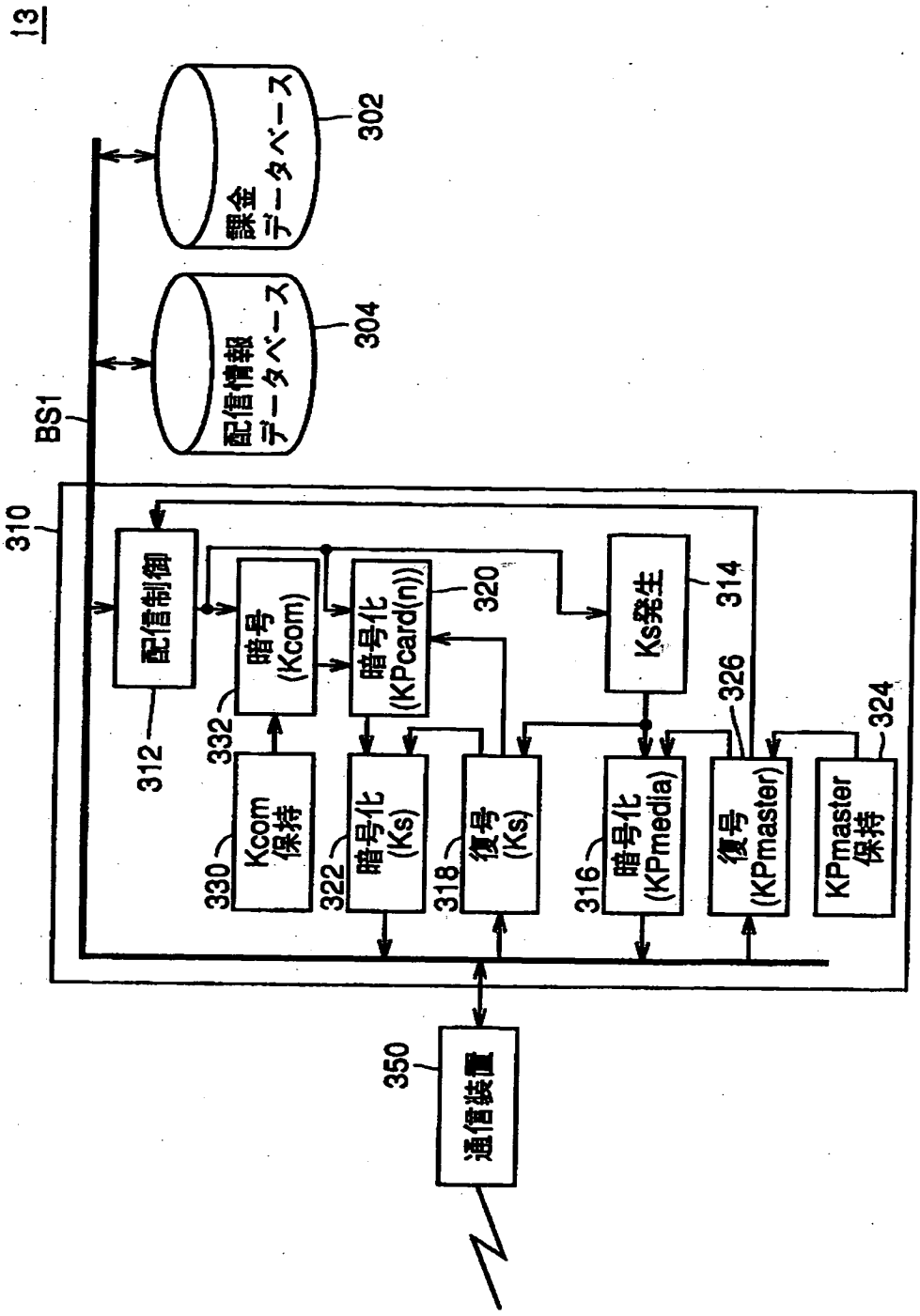
【図４３】


S511から
S538から
ライセンスキーKcを配信情報データベースより取得
S540
キーKPcard(1)により、キーKc、データLicenseを暗号化
S542
キーKs1により[Kc,License]Kcard(1)を暗号化
S544
[[Kc,License]Kcard(1)]Ks1を送信
S546
Ks1により復号化
S550
データ[Kc,License]Kcard(1)をメモリに記録
S552
Kcard(1)により[Kc,License]Kcard(1)を復号、データLicenseをレジスタに格納
S554
管理データベースに異常終了記録を格納
S561
販売機にて配信受理を受信
S558
管理データベースに販売記録を格納
S560
終了
S562

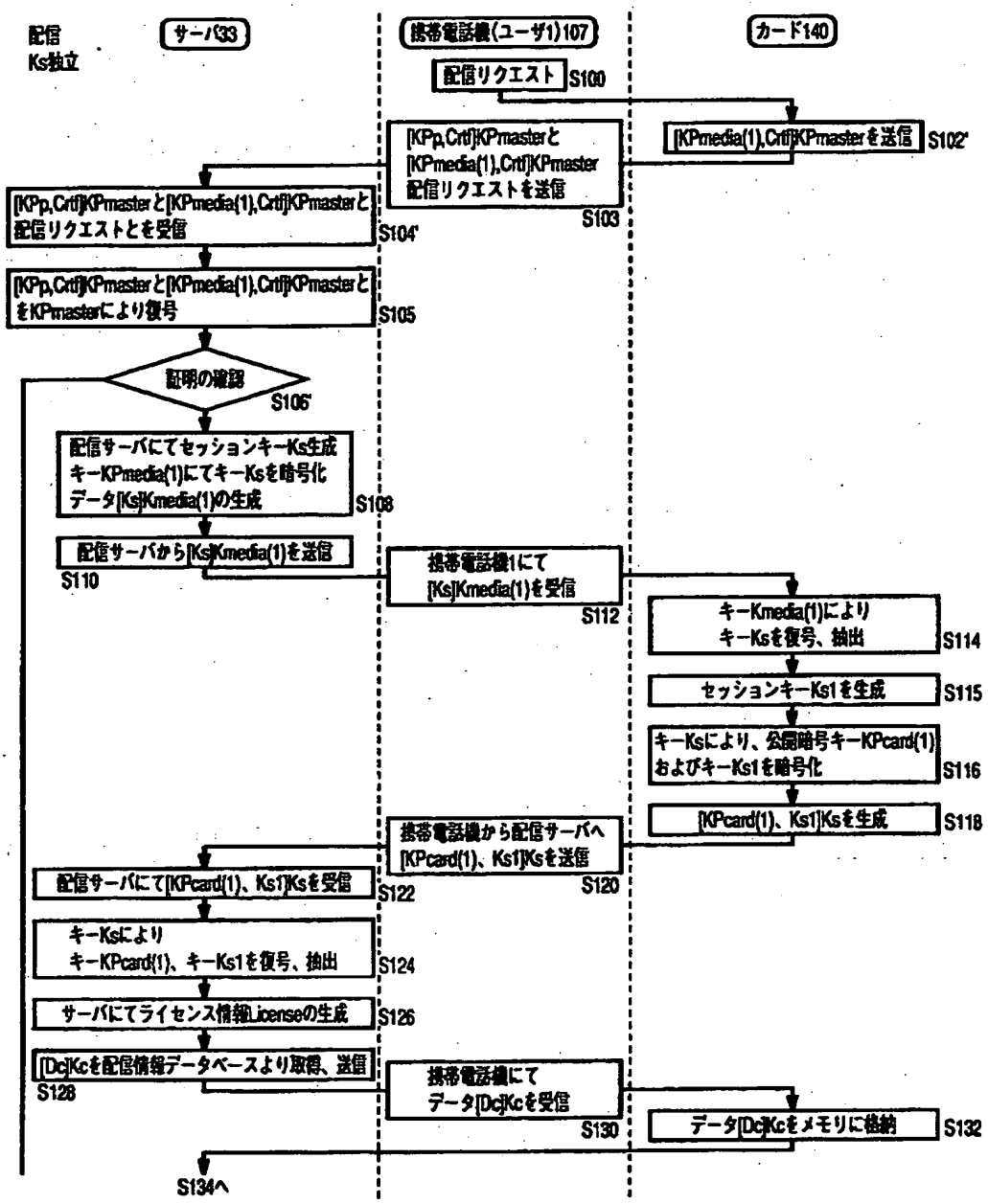
【図４４】


107
1514
1512
DA
1506
復号 Ks
[KPp,Crtf]KPmaster保持
1525
暗号化
1504
Ks発生
1502
復号 Kp
1522
Kp保持
1520
1530
Kcom
1532
復号 Kcom
メモリ インターフェース
1200
メモリカード
140
1510
混合
1508
音楽再生
1112
音声再生
ディスプレイ
1110
1108
キー
コントローラ
1106
1104
送受信
1102
BS2

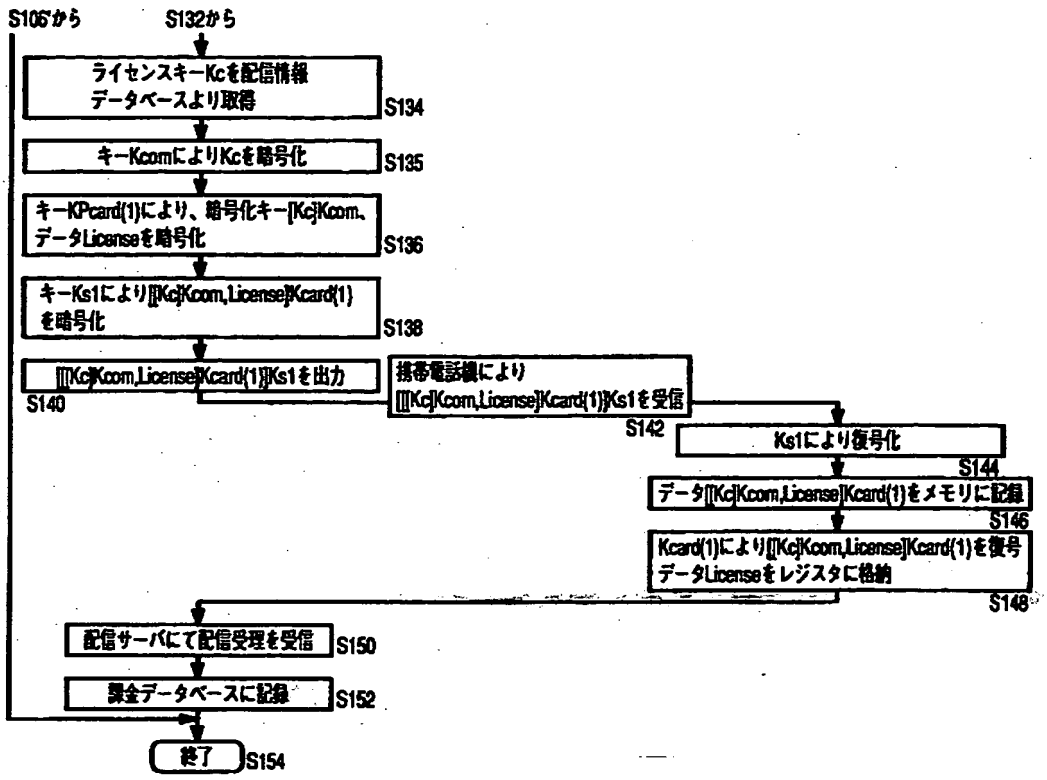
【図４５】


13
課金データベース
302
配信情報データベース
304
BS1
310
配信制御
312
暗号(Kcom)
332
暗号化(KPcard(n))
320
Ks発生
314
326
324
Kcom保持
330
暗号化(Ks)
322
復号(Ks)
318
暗号化(KPmedia)
316
復号(KPmaster)
KPmaster保持
通信装置
350

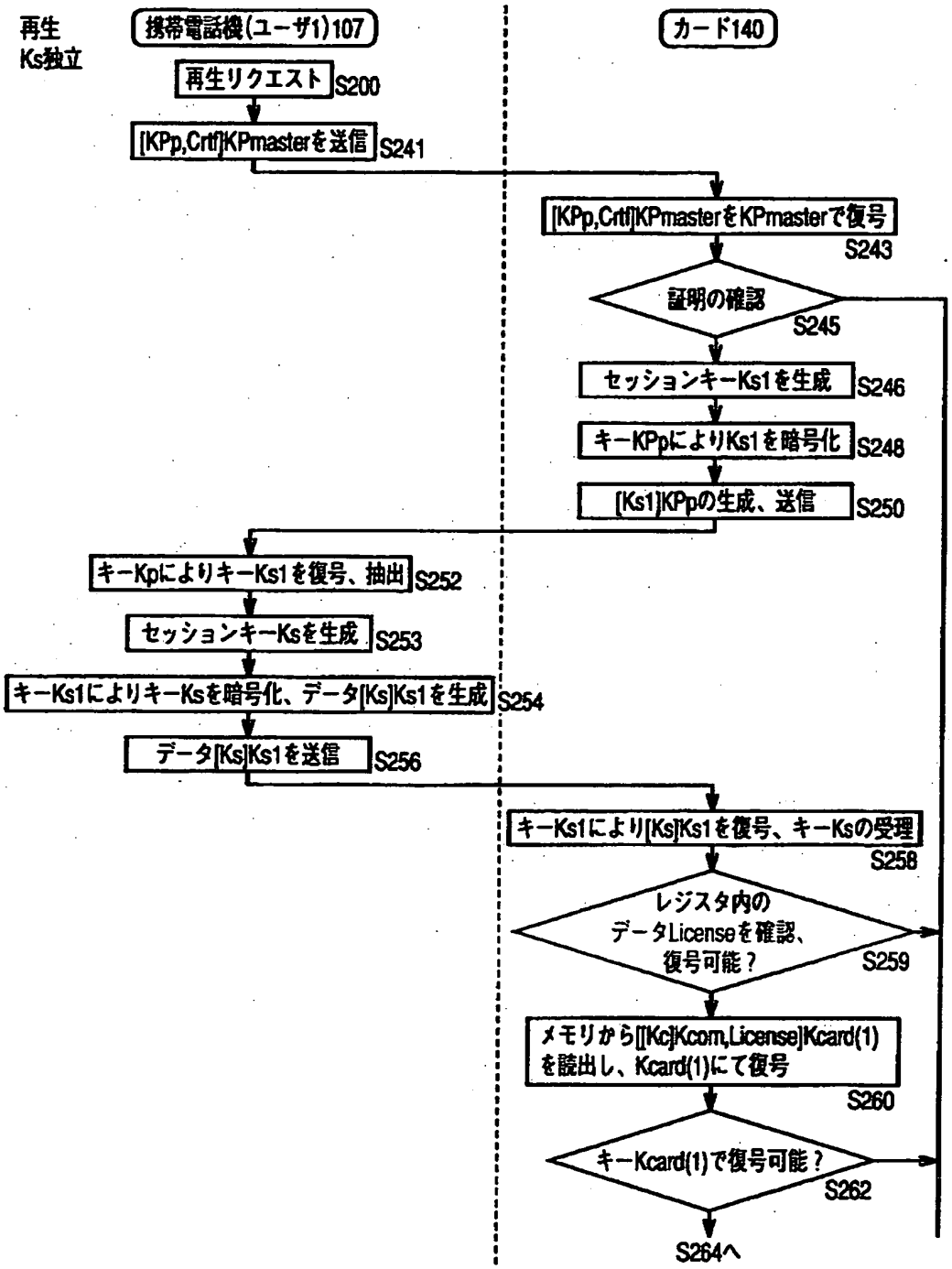
【図４６】


配信
Ks独立
サーバ33
携帯電話機(ユーザ1)107
カード140
配信リクエスト S100
[KPp,Crtf]KPmasterと
[KPmedia(1),Crtf]KPmaster
配信リクエストを送信
S103
[KPmedia(1),Crtf]KPmasterを送信 S102'
[KPp,Crtf]KPmasterと[KPmedia(1),Crtf]KPmasterと
配信リクエストとを受信 S104'
[KPp,Crtf]KPmasterと[KPmedia(1),Crtf]KPmasterと
をKPmasterにより復号 S105
証明の確認 S106'
配信サーバにてセッションキーKs生成
キーKPmedia(1)にてキーKsを暗号化
データ[Ks]Kmedia(1)の生成 S108
配信サーバから[Ks]Kmedia(1)を送信
S110
携帯電話機1にて
[Ks]Kmedia(1)を受信
S112
キーKmedia(1)により
キーKsを復号、抽出 S114
セッションキーKs1を生成 S115
キーKsにより、公開暗号キーKPcard(1)
およびキーKs1を暗号化 S116
[KPcard(1)、Ks1]Ksを生成 S118
携帯電話機から配信サーバへ
[KPcard(1)、Ks1]Ksを送信
S120
配信サーバにて[KPcard(1)、Ks1]Ksを受信
S122
キーKsにより
キーKPcard(1)、キーKs1を復号、抽出 S124
サーバにてライセンス情報Licenseの生成 S126
[Dc]Kcを配信情報データベースより取得、送信
S128
携帯電話機にて
データ[Dc]Kcを受信
S130
データ[Dc]Kcをメモリに格納 S132
S134へ

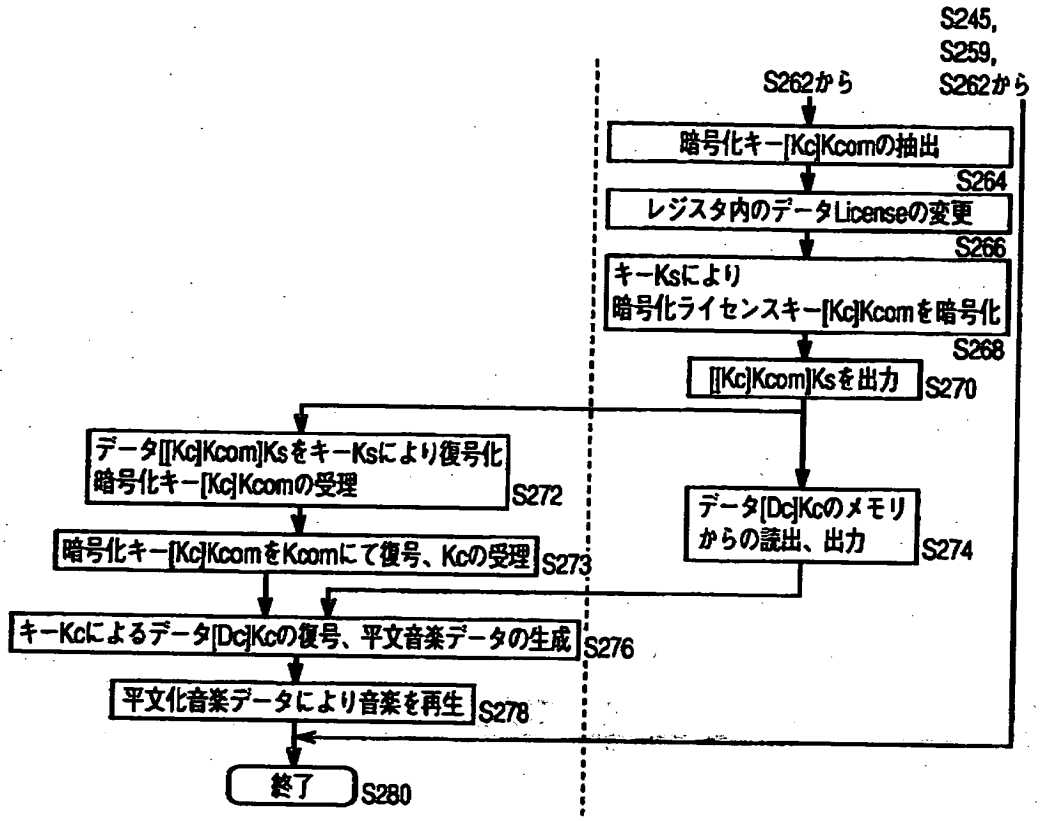
【図４７】


S105'から
S132から
ライセンスキーKcを配信情報データベースより取得
S134
キーKcomによりKcを暗号化
S135
キーKPcard(1)により、暗号化キー[Kc]Kcom、データLicenseを暗号化
S136
キーKs1により[[Kc]Kcom,License]Kcard(1)を暗号化
S138
[[Kc]Kcom,License]Kcard(1)]Ks1を出力
S140
携帯電話機により[[Kc]Kcom,License]Kcard(1)]Ks1を受信
S142
Ks1により復号化
S144
データ[[Kc]Kcom,License]Kcard(1)をメモリに記録
S146
Kcard(1)により[[Kc]Kcom,License]Kcard(1)を復号
データLicenseをレジスタに格納
S148
配信サーバにて配信受理を受信
S150
課金データベースに記録
S152
終了
S154

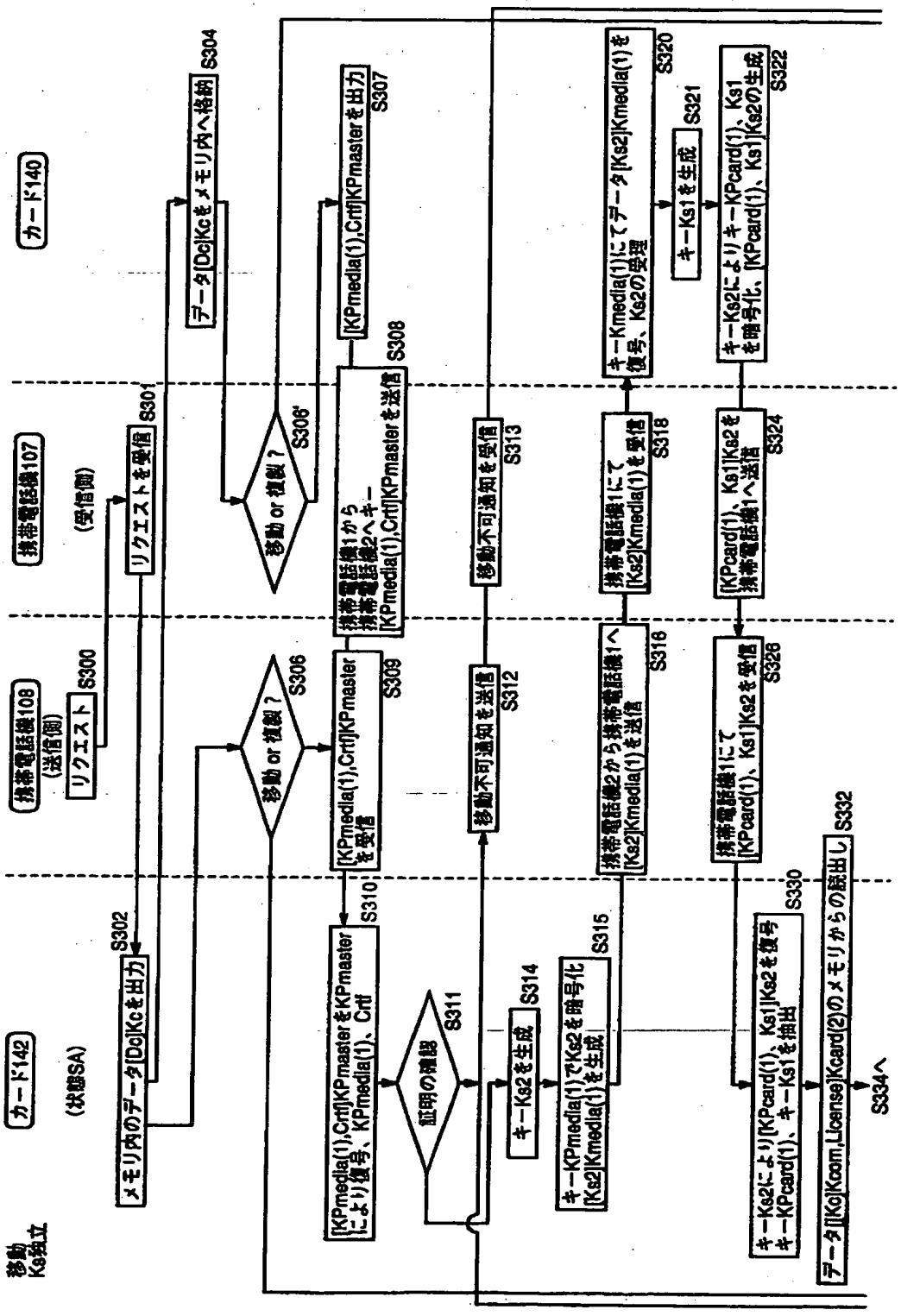
【図４８】


再生
Ks独立
携帯電話機(ユーザ1)107
カード140
再生リクエスト S200
[KPp,Crtf]KPmasterを送信 S241
[KPp,Crtf]KPmasterをKPmasterで復号 S243
証明の確認 S245
セッションキーKs1を生成 S246
キーKPpによりKs1を暗号化 S248
[Ks1]KPpの生成、送信 S250
キーKpによりキーKs1を復号、抽出 S252
セッションキーKsを生成 S253
キーKs1によりキーKsを暗号化、データ[Ks]Ks1を生成 S254
データ[Ks]Ks1を送信 S256
キーKs1により[Ks]Ks1を復号、キーKsの受理 S258
レジスタ内の
データLicenseを確認、
復号可能？ S259
メモリから[[Kc]Kcom,License]Kcard(1)
を読出し、Kcard(1)にて復号 S260
キーKcard(1)で復号可能？ S262
S264へ

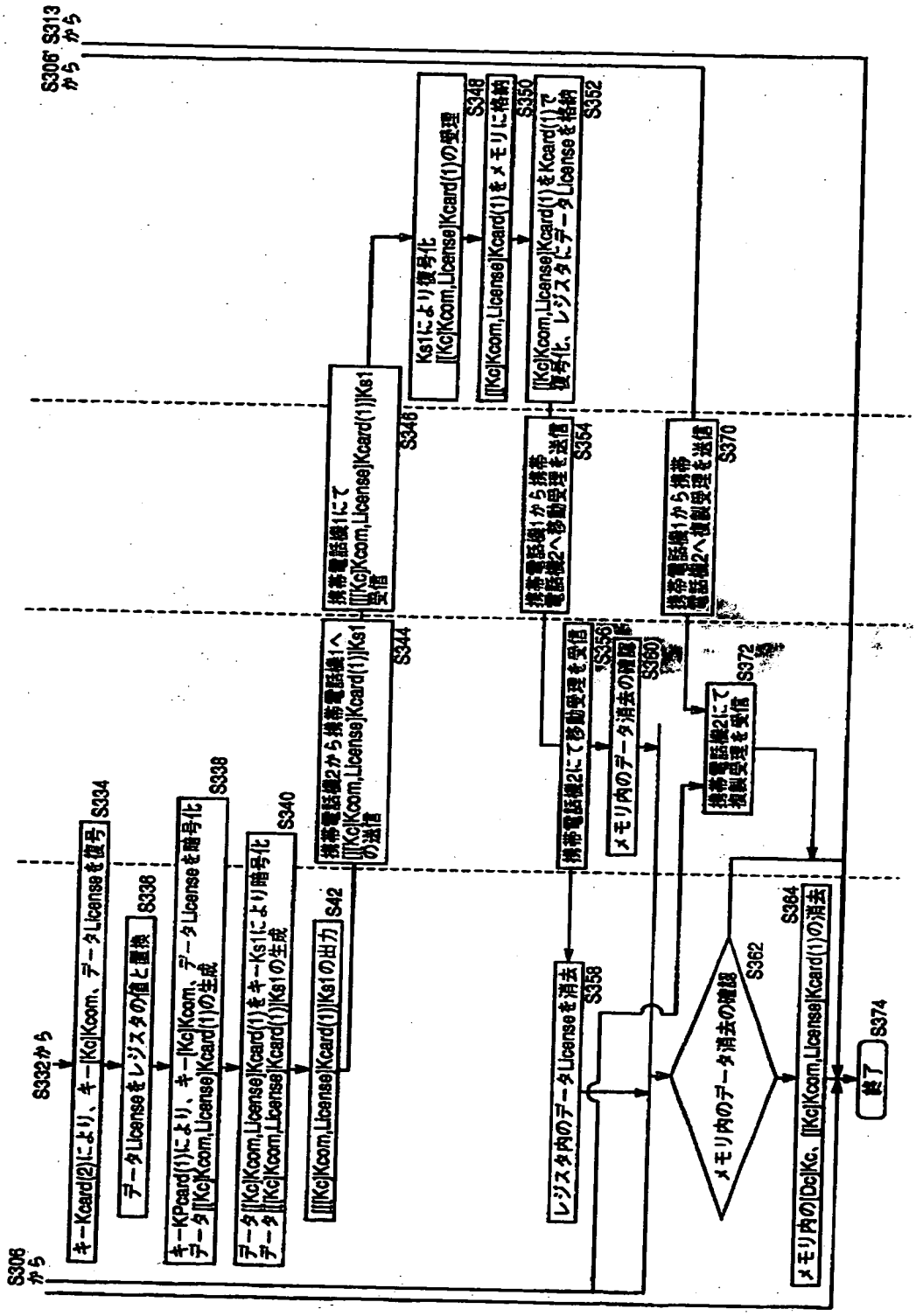
【図４９】


S245,
S259,
S262から
S262から
暗号化キー[Kc]Kcomの抽出
S264
レジスタ内のデータLicenseの変更
S266
キーKsにより
暗号化ライセンスキー[Kc]Kcomを暗号化
S268
[[Kc]Kcom]Ksを出力
S270
データ[[Kc]Kcom]Ksをキー Ksにより復号化
暗号化キー[Kc]Kcomの受理
S272
暗号化キー[Kc]KcomをKcomにて復号、Kcの受理
S273
データ[Dc]Kcのメモリ
からの読出、出力
S274
キーKcによるデータ[Dc]Kcの復号、平文音楽データの生成
S276
平文化音楽データにより音楽を再生
S278
終了
S280

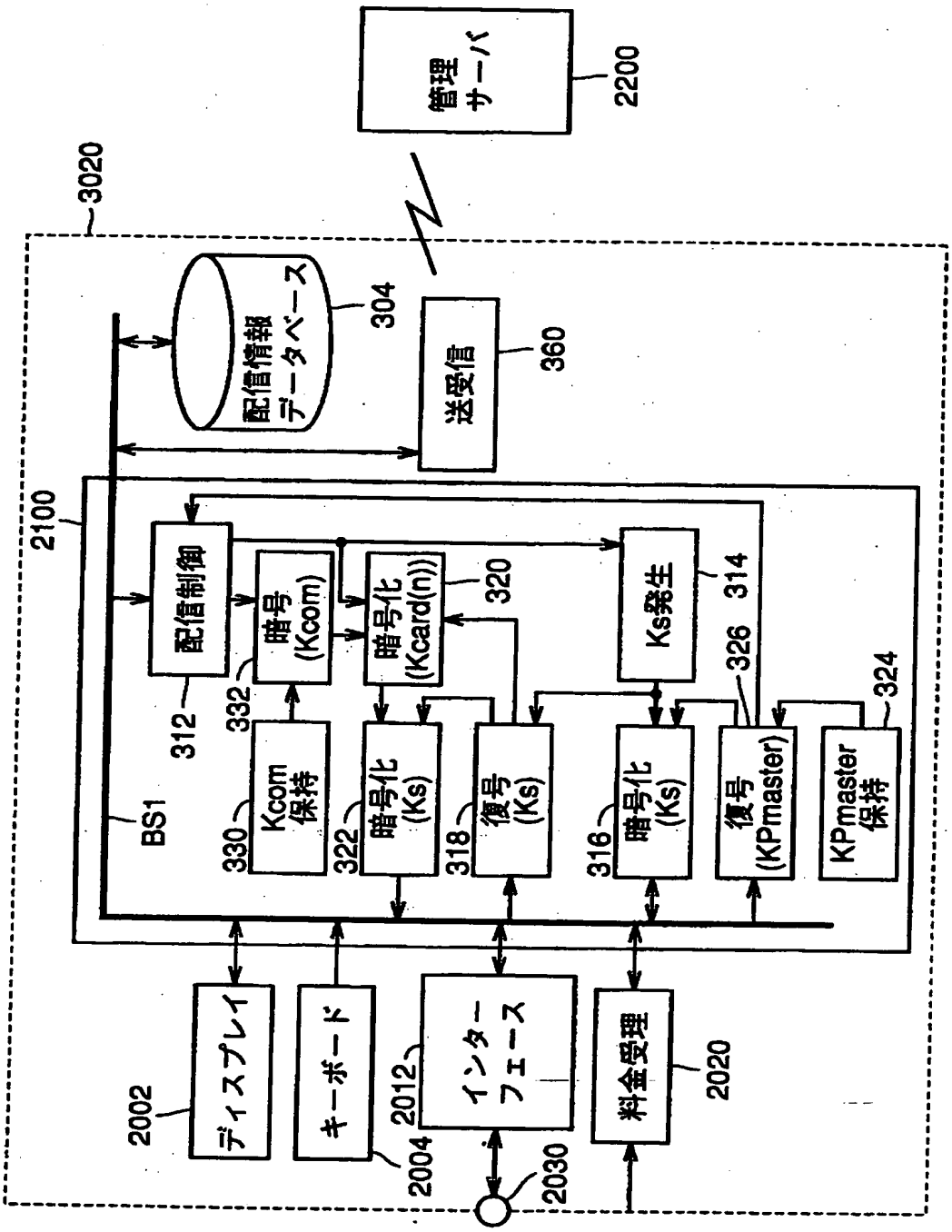
【図５０】


移動
Ks独立
カード142
(状態SA)
携帯電話機108
(送信側)
携帯電話機107
(受信側)
カード140
リクエスト
S300
リクエストを受信
S301
メモリ内のデータ[Do]Kcを出力
S302
データ[Do]Kcをメモリ内へ格納
S304
移動 or 複製 ?
S306
S306'
[KPmedia(1),Crtf]KPmasterを出力
S307
携帯電話機1から
携帯電話機2へキー
[KPmedia(1),Crtf]KPmasterを送信
S308
[KPmedia(1),Crtf]KPmaster
を受信
S309
[KPmedia(1),Crtf]KPmasterをKPmaster
により復号、KPmedia(1)、Crtf
S310
移動不可通知を送信
S312
移動不可通知を受信
S313
証明の確認
S311
キーKs2を生成
S314
キーKPmedia(1)でKs2を暗号化
[Ks2]Kmedia(1)を生成
S315
携帯電話機2から携帯電話機1へ
[Ks2]Kmedia(1)を送信
S316
携帯電話機1にて
[Ks2]Kmedia(1)を受信
S318
キーKmedia(1)にてデータ[Ks2]Kmedia(1)を
復号、Ks2の受理
S320
キーKs1を生成
S321
キーKs2によりキーKPcard(1)、Ks1
を暗号化、[KPcard(1)、Ks1]Ks2の生成
S322
[KPcard(1)、Ks1]Ks2を
携帯電話機1へ送信
S324
携帯電話機1にて
[KPcard(1)、Ks1]Ks2を受信
S326
キーKs2により[KPcard(1)、Ks1]Ks2を復号
キーKPcard(1)、キーKs1を抽出
S330
データ[[Ko]Kcom,License]Kcard(2)のメモリからの読出し
S332
S334へ

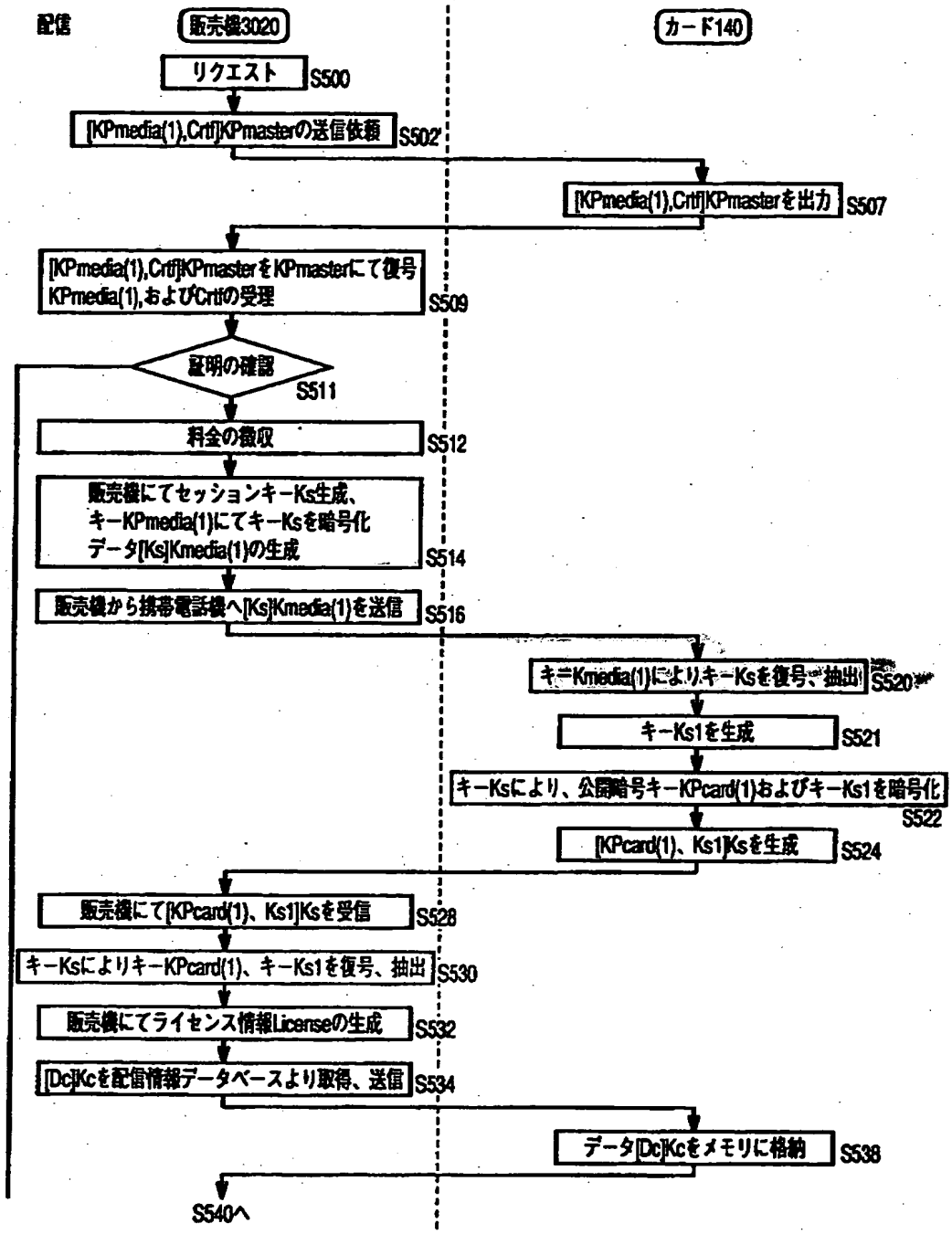
【図５１】


S306から
S332から
キーKcard(2)により、キーKc|Kcom、データLicenseを復号
S334
データLicenseをレジスタの値と置換
S338
キーKPcard(1)により、キーKc|Kcom、データLicenseを暗号化
データKc|Kcom,License|Kcard(1)の生成
S338
データKc|Kcom,License|Kcard(1)をキーKs1により暗号化
データKc|Kcom,License|Kcard(1)Ks1の生成
S340
Kc|Kcom,License|Kcard(1)Ks1の出力
S42
携帯電話機2から携帯電話機1へ
Kc|Kcom,License|Kcard(1)Ks1
の送信
S344
携帯電話機1にて
Kc|Kcom,License|Kcard(1)Ks1
受信
S346
Ks1により復号化
Kc|Kcom,License|Kcard(1)の受理
S348
Kc|Kcom,License|Kcard(1)をメモリに格納
S350
Kc|Kcom,License|Kcard(1)をKcard(1)で
復号化、レジスタにデータLicenseを格納
S352
携帯電話機1から携帯
電話機2へ移動受理を送信
S354
携帯電話機2にて移動受理を受信
S356
メモリ内のデータ消去の確認
S360
携帯電話機1から携帯
電話機2へ複製受理を送信
S370
携帯電話機2にて
複製受理を受信
S372
レジスタ内のデータLicenseを消去
S358
メモリ内のデータ消去の確認
S362
メモリ内のDc|Kc、Kc|Kcom,License|Kcard(1)の消去
S364
終了
S374

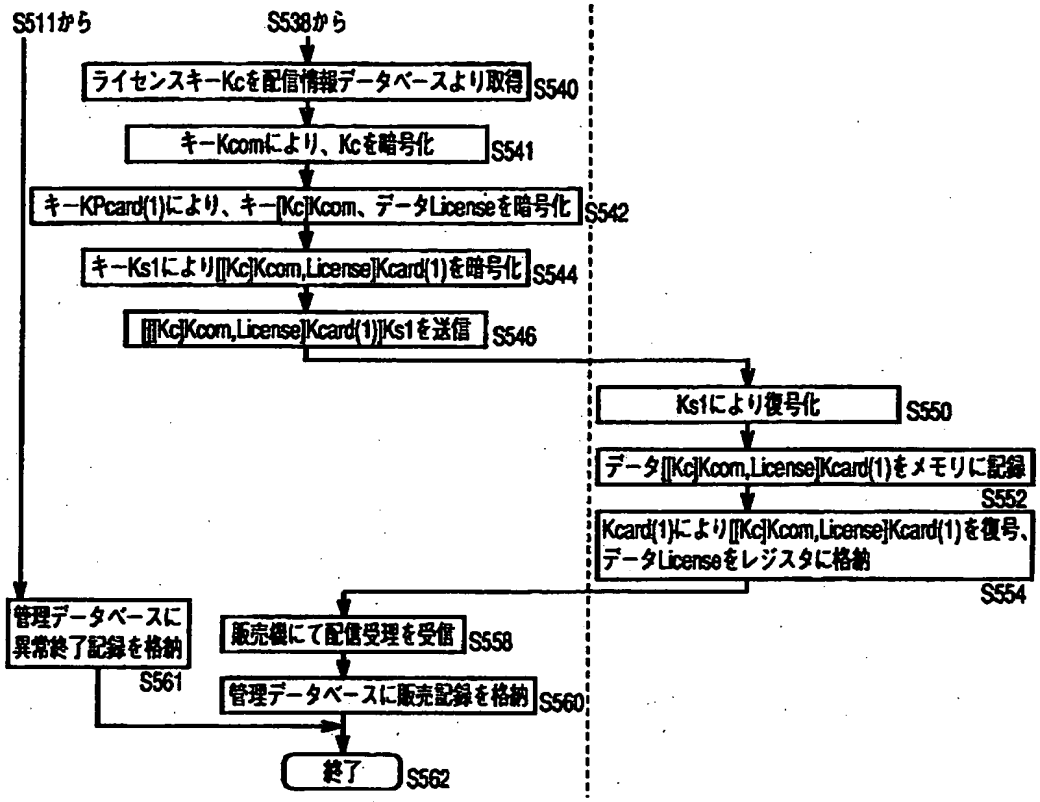
【図５２】


管理サーバ
2200
3020
配信情報データベース
304
送受信
360
2100
配信制御
312
暗号(Kcom)
332
暗号化(Kcard(n))
320
Ks発生
314
326
324
BS1
Kcom保持
330
暗号化(Ks)
322
復号(Ks)
318
暗号化(Ks)
316
復号(KPmaster)
KPmaster保持
ディスプレイ
2002
キーボード
2004
インターフェース
2012
料金受理
2020
2030

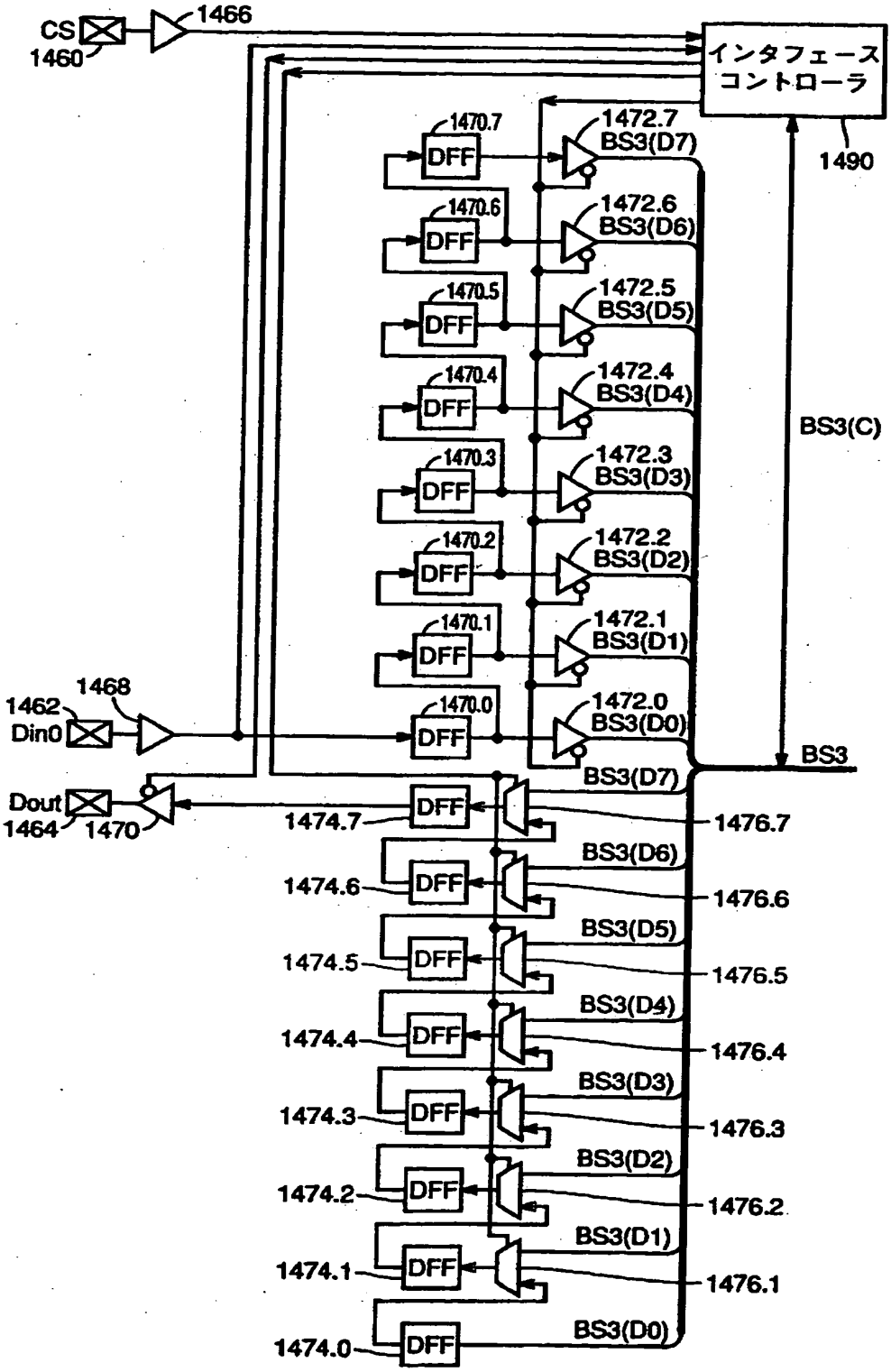
【図５３】


配信
販売機3020
カード140
リクエスト
S500
[KPmedia(1),Crtf]KPmasterの送信依頼
S502
[KPmedia(1),Crtf]KPmasterを出力
S507
[KPmedia(1),Crtf]KPmasterをKPmasterにて復号
KPmedia(1),およびCrtfの受理
S509
証明の確認
S511
料金の徴収
S512
販売機にてセッションキーKs生成、
キーKPmedia(1)にてキーKsを暗号化
データ[Ks]Kmedia(1)の生成
S514
販売機から携帯電話機へ[Ks]Kmedia(1)を送信
S516
キーKmedia(1)によりキーKsを復号、抽出
S520
キーKs1を生成
S521
キーKsにより、公開暗号キーKPcard(1)およびキーKs1を暗号化
S522
[KPcard(1)、Ks1]Ksを生成
S524
販売機にて[KPcard(1)、Ks1]Ksを受信
S528
キーKsによりキーKPcard(1)、キーKs1を復号、抽出
S530
販売機にてライセンス情報Licenseの生成
S532
[Dc]Kcを配信情報データベースより取得、送信
S534
データ[Dc]Kcをメモリに格納
S538
S540へ

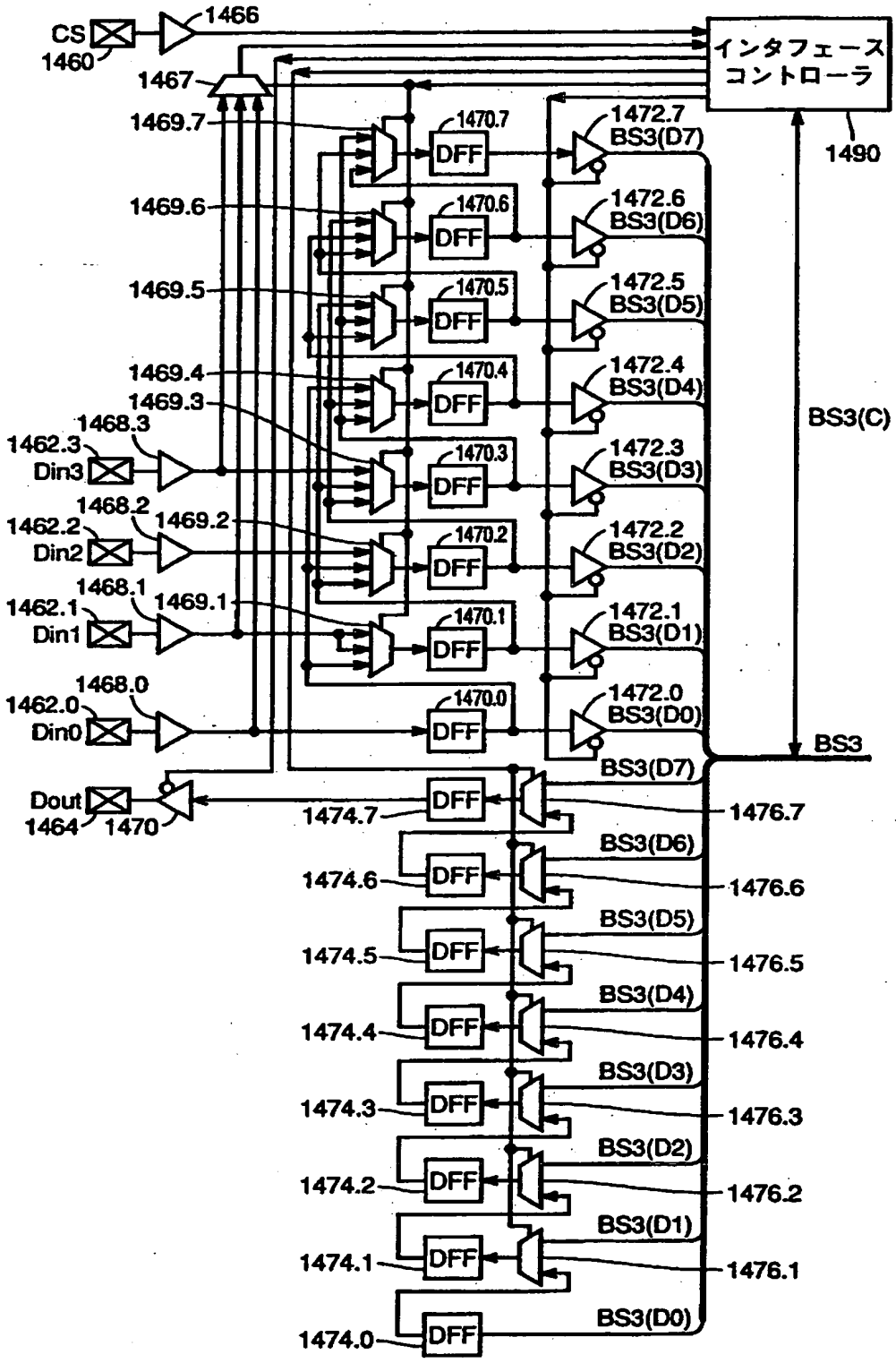
【図５４】


S511から
S538から
ライセンスキーKcを配信情報データベースより取得
S540
キーKcomにより、Kcを暗号化
S541
キーKPcard(1)により、キー[Kc]Kcom、データLicenseを暗号化
S542
キーKs1により[[Kc]Kcom,License]Kcard(1)を暗号化
S544
[[Kc]Kcom,License]Kcard(1)]Ks1を送信
S546
Ks1により復号化
S550
データ[[Kc]Kcom,License]Kcard(1)をメモリに記録
S552
Kcard(1)により[[Kc]Kcom,License]Kcard(1)を復号、
データLicenseをレジスタに格納
S554
管理データベースに
異常終了記録を格納
S561
販売機にて配信受理を受信
S558
管理データベースに販売記録を格納
S560
終了
S562

【図５５】


CS
1460
1466
インタフェース
コントローラ
1490
1470.7
DFF
1472.7
BS3(D7)
1470.6
DFF
1472.6
BS3(D6)
1470.5
DFF
1472.5
BS3(D5)
1470.4
DFF
1472.4
BS3(D4)
BS3(C)
1470.3
DFF
1472.3
BS3(D3)
1470.2
DFF
1472.2
BS3(D2)
1470.1
DFF
1472.1
BS3(D1)
1468
1462
Din0
1470.0
DFF
1472.0
BS3(D0)
BS3
BS3(D7)
Dout
1464
1470
1474.7
DFF
1476.7
BS3(D6)
1474.6
DFF
1476.6
BS3(D5)
1474.5
DFF
1476.5
BS3(D4)
1474.4
DFF
1476.4
BS3(D3)
1474.3
DFF
1476.3
BS3(D2)
1474.2
DFF
1476.2
BS3(D1)
1474.1
DFF
1476.1
1474.0
DFF
BS3(D0)

【図５６】


CS
1460
1466
1467
インタフェース
コントローラ
1490
1469.7
1470.7
DFF
1472.7
BS3(D7)
1469.6
1470.6
DFF
1472.6
BS3(D6)
1469.5
1470.5
DFF
1472.5
BS3(D5)
1469.4
1470.4
DFF
1472.4
BS3(D4)
1469.3
BS3(C)
1468.3
1462.3
Din3
1470.3
DFF
1472.3
BS3(D3)
1468.2
1462.2
Din2
1469.2
1470.2
DFF
1472.2
BS3(D2)
1468.1
1462.1
Din1
1469.1
1470.1
DFF
1472.1
BS3(D1)
1468.0
1462.0
Din0
1470.0
DFF
1472.0
BS3(D0)
BS3
BS3(D7)
Dout
1464
1470
1474.7
DFF
1476.7
BS3(D6)
1474.6
DFF
1476.6
BS3(D5)
1474.5
DFF
1476.5
BS3(D4)
1474.4
DFF
1476.4
BS3(D3)
1474.3
DFF
1476.3
BS3(D2)
1474.2
DFF
1476.2
BS3(D1)
1474.1
DFF
1476.1
BS3(D0)
1474.0
DFF

【書類名】　　要約書

【要約】

【課題】　著作権者の許可なく複製されることを防止することが可能な情報配信システムを提供する。

【解決手段】　メモリカード１１０は、サーバから携帯電話網を介してデータバスＢＳ３に与えられるデータから、復号処理をすることによりセッションキーＫｓを抽出する。暗号化処理部１４０６は、セッションキーＫｓに基づいて、メモリカード１１０の公開暗号化鍵ＫＰｃａｒｄ（１）を暗号化してデータバスＢＳ３を介してサーバに与える。レジスタ１５００は、復号されたライセンスＩＤ、ユーザＩＤ等のデータをサーバから受けとって格納し、メモリ１４１２は、データバスＢＳ３からライセンスキーＫｃにより暗号化されている暗号化コンテンツデータ［Ｄｃ］Ｋｃを受けて格納する。

【選択図】　　図５

認定・付加情報

特許出願の番号	平成１１年　特許願　第３４５２２９号
受付番号	５９９０１１８３９９８
書類名	特許願
担当官	塩崎　博子　　１６０６
作成日	平成１２年　２月１０日

＜認定情報・付加情報＞

【特許出願人】
　【識別番号】　000005223
　【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号
　【氏名又は名称】　富士通株式会社
【特許出願人】
　【識別番号】　000005108
　【住所又は居所】　東京都千代田区神田駿河台四丁目６番地
　【氏名又は名称】　株式会社日立製作所
【特許出願人】
　【識別番号】　000004167
　【住所又は居所】　東京都港区赤坂４丁目１４番１４号
　【氏名又は名称】　日本コロムビア株式会社
【特許出願人】
　【識別番号】　000001889
　【住所又は居所】　大阪府守口市京阪本通２丁目５番５号
　【氏名又は名称】　三洋電機株式会社
【代理人】　申請人
　【識別番号】　100064746
　【住所又は居所】　大阪府大阪市北区南森町２丁目１番２９号　住友銀行南森町ビル　深見特許事務所
　【氏名又は名称】　深見　久郎
【選任した代理人】
　【識別番号】　100085132
　【住所又は居所】　大阪府大阪市北区南森町２丁目１番２９号　住友銀行南森町ビル　深見特許事務所
　【氏名又は名称】　森田　俊雄
【選任した代理人】
　【識別番号】　100091409

次頁有

認定・付加情報（続き）

【住所又は居所】　大阪府大阪市北区南森町２－１－２９　住友銀行南森町ビル　深見特許事務所
【氏名又は名称】　伊藤　英彦
【選任した代理人】
【識別番号】　100096781
【住所又は居所】　大阪府大阪市北区南森町２－１－２９　住友銀行南森町ビル　深見特許事務所
【氏名又は名称】　堀井　豊

次頁無

出　願　人　履　歴　情　報

識別番号　　〔０００００５２２３〕

１．変更年月日　　１９９６年　３月２６日
　［変更理由］　　住所変更
　　住　所　　神奈川県川崎市中原区上小田中４丁目１番１号
　　氏　名　　富士通株式会社

出 願 人 履 歴 情 報

識別番号　〔０００００５１０８〕

１．変更年月日　１９９０年　８月３１日
［変更理由］　新規登録
住　所　東京都千代田区神田駿河台４丁目６番地
氏　名　株式会社日立製作所

出　願　人　履　歴　情　報

識別番号　　〔０００００４１６７〕

１．変更年月日　　１９９０年　８月２１日
［変更理由］　新規登録
住　所　東京都港区赤坂４丁目１４番１４号
氏　名　日本コロムビア株式会社

出 願 人 履 歴 情 報

識別番号　〔０００００１８８９〕

１．変更年月日　１９９３年１０月２０日
［変更理由］　住所変更
住　所　大阪府守口市京阪本通２丁目５番５号
氏　名　三洋電機株式会社